

TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ
Európsky fond regionálneho rozvoja



Čiastková štúdia uskutočniteľnosti projektov prioritnej osi č.1
Elektronizácia verejnej správy a rozvoja elektronických služieb
Operačného programu Informatizácia spoločnosti

Dátové centrum pre eGovernment

Obsah

1	Základné informácie	1
1.1	Úvod	1
1.2	Prehľad	1
1.3	Dôvod	1
1.4	Rozsah	2
1.5	Rámec projektu	3
1.6	Použité skratky a značky	3
2	Manažérske zhrnutie	5
3	Popis aktuálneho stavu	7
3.1	Legislatívna analýza	7
3.2	Biznis architektúra	8
3.2.1	Konsolidácia IKT pre organizácie štátnej správy	8
3.2.2	Projekty PO1 OPIS	8
3.2.3	Dátové centrá vo verejnej správe SR	8
3.2.4	Súčasný a predpokladaný využitie infraštruktúry DataCentra pre iné rezorty	9
3.3	Aplikačná a dátová architektúra	10
3.3.1	DataCentrum	10
3.3.2	Ministerstvo vnútra SR	11
3.4	Infraštruktúra	12
3.4.1	DataCentrum	12
3.4.2	Ministerstvo vnútra SR	15
3.5	Bezpečnostná analýza	17
3.5.1	Legislatívne východiská	18
4	Popis cieľového stavu	20
4.1	Legislatívna analýza	20
4.2	Analýza požiadaviek a potrieb stakeholderov	20
4.2.1	Rozvoj komunikačno-technickej infraštruktúry ISVS na centrálnej úrovni	21
4.3	Popis navrhovaného riešenia	24
4.3.1	Biznis architektúra	24
4.3.2	Aplikačná a dátová architektúra	38
4.3.3	Infraštruktúra	41
4.4	Definície služieb	53
4.5	Uskutočniteľnosť a náklady	54
4.5.1	Dopady na technické a softwarové vybavenie	54
4.5.2	Organizačné dopady	54
4.5.3	Legislatívne dopady	56
4.5.4	Prevádzkové a bezpečnostné dopady	57
4.5.5	Nasadenie riešenia a marketingové požiadavky	60

4.5.6	Cena riešenia	60
4.6	Ekonomická analýza	66
4.6.1	Strategický kontext	67
4.6.2	Ciele a obmedzenia	67
4.6.3	Stručný popis alternatívnych riešení	68
4.6.4	Kvantitatívna analýza navrhnutého riešenia	68
4.6.5	Analýza rizík	70
4.6.6	Nefinančné prínosy a náklady	74
4.7	Návrh projektového zámeru	75
4.7.1	Príprava projektu	75
4.7.2	Metodika riadenia	75
4.7.3	Harmonogram projektu	77
5	Prílohy	79
5.1	Kalkulácia celkových nákladov na vlastníctvo softvéru (TCO)	79
5.2	Kalkulácia nákladov na vlastníctvo hardvéru	79

1 Základné informácie

1.1 Úvod

Štúdia vychádza zo štúdie „Národný projekt Centrálna služba dátového centra pre elektronizáciu verejnej správy“ vypracovanej pre Ministerstvo financií Slovenskej republiky spoločnosťou Arthur D. Little.

Pôvodná štúdia bola upravená a rozšírená tak, aby reflektovala aktuálny stav operačného programu OPIS a organizačného, procesného aj technického vybavenia DataCentra (rozpočtová organizácia, ktorej zriaďovateľom je Ministerstvo financií SR) a Ministerstva vnútra SR.

Štúdia je vypracovaná na základe vzoru štúdie pre projekty prioritnej osi 1 operačného programu OPIS.

1.2 Prehľad

Predložený dokument bol spracovaný na základe požiadavky DataCentra. Cieľom štúdie uskutočniteľnosti je posúdiť technickú, organizačnú a finančnú rovinu implementácie a prevádzky nadrezortného Dátového centra ako poskytovateľa centrálnych služieb dátového centra pre elektronizáciu verejnej správy.

Financovanie budovania Dátového centra sa predpokladá zo zdrojov Operačného programu informatizácie spoločnosti, z hľadiska ktorého predstavuje projekt až do odovzdania do rutinej prevádzky oprávnený náklad.

Štúdia predpokladá budovanie Dátového centra v pôsobnosti dvoch organizácií DataCentrum a Ministerstvo vnútra SR. Datacentrum má vzhľadom na postavenie svojho zriaďovateľa (Ministerstvo financií SR) v informatizácii spoločnosti a svoje konkrétne poslanie v rámci týchto aktivít veľmi dobré predpoklady pre zrealizovanie tejto úlohy. DataCentrum v zmysle svojho štatútu koordinuje, gesturuje a metodicky usmerňuje tvorbu koncepcie rozvoja informačného systému rezortu, rozvoj informačného systému rezortu MF SR a jeho častí v procese jeho tvorby, aktualizácie a realizácie. Formuluje štandardy, metodické, organizačné a legislatívne podmienky pre integráciu, vzájomnú prepojitelnosť častí informačného systému rezortu MF SR a pre bezpečnosť informačného systému rezortu MF SR. Ministerstvo vnútra SR má v informatizácii slovenskej verejnej správy taktiež významnú úlohu, spravuje a prevádzkuje niekoľko kritických ISVS, viacero ISVS je v štádiu implementácie, pričom medzi ne patria aj základné komponenty celého eGovernmentu – základné registre.

1.3 Dôvod

Primárnym dôvodom spracovania štúdie je vyhodnotenie uskutočniteľnosti projektu vytvorenia centrálného nadrezortného poskytovateľa služieb dátového centra v rámci elektronizácie verejnej správy.

Požiadavka na elektronizáciu služieb verejnej správy bola schválená uznesením vlády SR č. 131/2008 v rámci dokumentu „Stratégia informatizácie verejnej správy“, ktorého víziou je

dosahovať neustály rast spokojnosti občanov s verejnou správou prostredníctvom poskytovania služieb atraktívnym a jednoduchým spôsobom za súčasného zvyšovania svojej efektívnosti, kompetentnosti a znižovania nákladov na verejnú správu.

Koncepcia nadrezortného poskytovateľa služieb dátového centra adresuje primárne požiadavku na znižovanie nákladov na verejnú správu nakoľko zabezpečuje unifikáciu prostredia pre prevádzku informačných systémov poskytujúcich eGov služby, optimalizuje využitie zdrojov, znižuje obstarávacie a prevádzkové náklady a zvyšuje efektívnosť manažmentu na všetkých úrovniach od prevádzky infraštruktúry až po manažment vzťahov. Dôležitou oblasťou, ktorú priamo rieši predložený koncept, sú služby pre zabezpečenie požadovanej miery dostupnosti a bezpečnosti pre eGov služby čo priamo prispieva k pozitívnej skúsenosti a vnímaniu služieb verejnej správy z pohľadu občana.

Hlavným cieľom štúdie je analyzovať a vyhodnotiť udržateľnosť nadrezortného Dátového centra ako alternatívu k decentralizovanému a individuálnemu prístupu k poskytovaniu služieb dátových centier. Z tohto pohľadu je celková efektívnosť navrhovaného riešenia primárne závislá na miere využitia jeho služieb v rámci projektov PO1 OPIS, iných informačných systémov prevádzkovaných v rámci verejnej správy, resp. eliminácii budovania duplicitných poskytovateľov služieb dátových centier.

Vybudovanie plného nadrezortného dátového centra je komplexnou úlohou pozostávajúcou z viacerých krokov, ktoré v konečnom dôsledku budú viesť k existencii logického dátového centra pozostávajúceho z niekoľkých fyzických geograficky oddelených lokalít, organizačného a procesného zabezpečenia, a infraštruktúry na úrovni telekomunikácií, HW a SW, ktorá umožní transparentnú prevádzku pre organizácie prístupujúce k využívaniu služieb tohto dátového centra.

Primárnym cieľom tejto štúdie je zrealizovanie prvého kroku pri budovaní takého dátového centra a to je zabezpečenie vhodných budov pre dátové centrá a základnej technologickej infraštruktúry, ktorá je predpokladom na budúce prevádzkovanie dátového centra – najmä dostatočné napájanie, sieťová konektivita a chladenie pri dodržaní požadovanej fyzickej bezpečnosti, redundancie a škálovateľnosti.

1.4 Rozsah

Táto štúdia uskutočniteľnosti popisuje súčasný stav a rámcovo navrhuje budúce riešenie centrálnych služieb nadrezortného dátového centra pre elektronizáciu verejnej správy.

Koncept centrálného dátového centra (ďalej iba Dátové centrum) poskytuje konsolidované, efektívne riadené a finančne optimálne prostredie pre prevádzku informačných systémov verejnej správy čím priamo znižuje náklady na poskytovanie eGov služieb. Dátové centrum vďaka svojej robustnosti zároveň zabezpečuje požadovanú dostupnosť a bezpečnosť eGov služieb.

Úvodnú časť štúdie tvorí analýza súčasného stavu zameraná primárne na prostredie DataCentra, ktoré už v súčasnosti poskytuje služby dátového centra aj mimo rezortu Ministerstva financií SR a prostredie Ministerstva vnútra SR.

Jadrom štúdie je návrh riešenia, ktorý pozostáva z procesnej, technickej a organizačnej časti. V časti biznis architektúry je návrh základného procesného modelu riadenia prevádzky dátového centra a identifikácia kľúčových služieb poskytovaných Dátovým centrom. V časti technického návrhu riešenia sú definované komponenty vysoko úrovňovej architektúry riešenia, v záverečnej časti návrhu riešenia sú definované systémy riadenia služieb a informačnej bezpečnosti vrátane vyžadovaného organizačného zabezpečenia.

Vo veľkej miere sa štúdia venuje cieľovému dátovému centru vrátane všetkých jeho aspektov. Pre navrhované prvé 2 projekty zo série krokov na jeho implementáciu obsahuje odhad nákladov na realizáciu projektu a finančnú analýzu navrhovaného riešenia. V časti projektového plánu je definovaná základná projektová organizácia, projektové aktivity a míľniky.

1.5 Rámec projektu

Táto štúdia uskutočniteľnosti sa opiera o nasledujúce dokumenty a literatúru:

- Operačný program informatizácia spoločnosti
- Stratégia informatizácie verejnej správy,
- Národná koncepcia informatizácie verejnej správy,
- Revízia budovania eGovernmentu (strednodobý plán implementácie priorít), prerokované a schválené Vládou SR dňa 2.2.2011
- Zákon č. 575/2001 Z.z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov
- Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy
- Výnos Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy, uverejnené v Z.z. č. 312/2010
- Ďalšie dokumenty a legislatívne predpisy popisované v rámci tohto dokumentu

1.6 Použité skratky a značky

Tabuľka 1 Vysvetlenie použitých skratiek a pojmov

Skratka / Značka	Vysvetlenie
CEP	Centrálny elektronický priečinok
DataCentrum	Organizácia v zriaďovateľskej pôsobnosti Ministerstva financií SR
Dátové centrum	Dátové centrum (uvádzané s veľkým "D"), ktoré je predmetom štúdie/projektu
DC	Dátové centrum
DNS	Domain name system/server
HW	Hardware
IaaS	Infrastructure as a service
IISVS	Integrovaný informačný systém verejnej správy
IKT	informačné a komunikačné technológie

ISVS	Informačný systém verejnej správy
IT	Informačné technológie
LAN	Local area network
MF SR	Ministerstvo financií Slovenskej republiky
MG	Motor generátor, náhradný zdroj elektrickej energie
MV SR	Ministerstvo vnútra Slovenskej republiky
NKIVS	Národná koncepcia informatizácie verejnej správy
OPIS	Operačný program Informatizácia spoločnosti
PaaS	Platform as a service
PDC	Primárne dátové centrum
PO1	Prioritná os 1
SaaS	Software as a service
SAN	Storage area network
SLA	Service level agreement
SW	Software
TCO	Total cost of ownership
UPS	Uninterruptible Power Supply - záložný zdroj
VPN	Virtual private network
WAN	Wide area network

2 Manažérske zhrnutie

V rámci projektov OPIS PO1 je predpokladaný rozvoj väčších alebo menších výpočtových stredísk, ktoré má dnes zriadené a prevádzkuje väčšina subjektov verejnej správy. Tieto zdroje sú už z historického hľadiska budované samostatne či už z pohľadu technologického alebo z pohľadu riadenia IKT, pričom tento stav viac menej pretrváva a aktuálne riešenie projektov OPIS tento stav konzervuje. Na druhej strane je ale potrebné povedať, že v súčasnosti badať tendencie smerujúce ku konsolidácii prostriedkov IKT na nadrezortnej úrovni. Ako príklad je možné spomenúť DataCentrum Ministerstva financií alebo koncepciu inteligentného regiónu Košice, v rámci ktorej je cieľom konsolidovať nie len zdroje IKT, ale aj technologické znalosti. DataCentrum sa stáva určitým konsolidačným prvkom aj z pohľadu prebiehajúcich projektov OPIS, na úrovni rezortnej – kde je plánovaná prevádzka systémov CEP v jeho priestoroch a aj na úrovni nadrezortnej, kde sa predpokladá hostovanie systému eHealth, Ministerstva zdravotníctva.

Všeobecne je možné konštatovať, že prostredie OPIS disponuje značným množstvom zdrojov na IKT infraštruktúru avšak v rámci súčasne plánovaného priebehu projektov ich nedokáže spoločne využiť. Každý projekt predpokladá vlastnú, redundantnú a vysoko dostupnú infraštruktúru v mnohých prípadoch s umiestnením v dvoch a niekedy až v troch geograficky oddelených lokalitách. Na túto infraštruktúru sú v rámci projektov dedikované nie malé finančné zdroje, pričom je potrebné zabezpečiť finančné zdroje aj na následnú prevádzku a podporu tejto infraštruktúry a v neposlednom rade aj na podporu používateľov eGov služieb. Súčasný stav zabezpečenia IKT infraštruktúry, jej prevádzky a podpory v prostredí projektov OPIS sa preto javí ako neoptimálny z hľadiska využitia plánovaných technických prostriedkov IKT.

Koncepcia IISVS popísaná v NKIVS, ktorá je základným rámcom pre projekty OPIS, kladie vysoké požiadavky na zabezpečenie dostupnosti, interoperability a bezpečnosti informačných systémov. Jednotlivé komponenty IISVS preto kladú nemalé nároky na vytvorenie zodpovedajúcej technologickej infraštruktúry spolu so zabezpečením jej prevádzky a podpory. Potrebné je preto koncepčným spôsobom riešiť jednak oblasť zabezpečenia budovaných eGov služieb nevyhnutnou IKT infraštruktúrou, tak aj zabezpečenie prevádzky a podpory tejto infraštruktúry.

Základnou myšlienkou tejto koncepcie je zabezpečenie centrálnych služieb dátového centra pre elektronizáciu verejnej správy, ktoré konsolidovaným spôsobom pokryjú požiadavky projektov informatizácie verejnej správy. Zo strategického hľadiska umožní takáto koncepcia vytvoriť prostredie pre budúci rozvoj eGov služieb tak, aby IKT pri rozvoji neboli obmedzujúcim faktorom ale vedeli pružne reagovať na budúce požiadavky a zmeny.

Vývoj v oblasti poskytovania IT služieb vo forme “Cloud Computing” otvára nové pole možností tým, že umožňuje jednoduchý prístup k dynamicky konfigurovateľným službám. Cloud predstavuje nový spôsob šetrenia IT nákladov formami, ktoré propagujú štandardné formy optimalizácie a zdieľania infraštruktúry, ako aj poskytovania unifikovaných služieb. Pre súčasný stav prevádzky a podpory v prostredí projektov OPIS je poskytovanie služieb formou Government Private Cloud-u spôsobom, ktorým sa eliminujú hlavné problémové faktory často

uvádzané pre Verejné Cloud-y (často iba Cloud-y) akými sú bezpečnosť, neznáma spoľahlivosť infraštruktúry a vlastníctvo dát.

Cieľovým stavom je stratégia formovania a správy infraštruktúry, ktorá nielen zabezpečí optimalizáciu kvality a nákladov z pohľadu krátkodobého, ale zároveň bude aj garantom jej udržateľnosti z hľadiska dlhodobého. Štúdia navrhuje riešenie dátových centier vo verejnej správe formou realizácie väčších dátových sál umožňujúcich dosiahnuť tieto ciele. Načrtáva aj rozloženie zodpovedností za prevádzku týchto dátových sál a IKT v nich prevádzkovaných a rámcový plán aktivít smerujúcich k ich realizácii.

Štúdia zároveň navrhuje a detailnejšie popisuje prvé 2 konkrétne kroky vyplývajúce z potrieb rozvoja infraštruktúry a aktuálnych podmienok na Slovensku, a to realizáciu dvoch dátových sál:

- sála prevádzkovaná DataCentrom v blízkosti Bratislavy
- sála prevádzkovaná Ministerstvom vnútra SR v blízkosti Banskej Bystrice

Parametre oboch dátových sál by mali vychádzať z úrovne Tier III (podľa metodiky The Uptime Institute). Štúdia ponúka analýzu rôznych možností prístupu k realizácii uvedených dátových sál spomedzi možností výstavby, adaptácie existujúcich priestorov a kúpy existujúcej dátovej sály (alebo jej časti). Ako najvhodnejšia možnosť v podmienkach DataCentra, resp. realizácie dátových sál v okolí Bratislavy, vzhľadom na finančnú, časovú efektivitu a riziká bola vyhodnotená kúpa časti existujúceho dátového centra disponujúceho potrebnou infraštruktúrou pre splnenie stanovených cieľov. V okolí Banskej Bystrice sa vzhľadom na neexistenciu vhodných priestorov dátových sál na kúpu a naopak existenciu vhodnej budovy vo vlastníctve MV SR na prebudovanie na dátové centrum ako najvhodnejší ukazuje práve variant adaptácie tejto budovy na dátové centrum.

3 Popis aktuálneho stavu

3.1 Legislatívna analýza

Legislatívny rámec je daný kompetenciami MF SR. Základné kompetencie ministerstva definuje zákon č. 575/2001 Z.z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

Ďalšie zákony, ktoré sú relevantné pre definované služby dátového centra sú v nasledovnej tabuľke:

Tabuľka 2 Kľúčové právne predpisy

Hlavné právne predpisy	
Číslo	Názov
Zákon č. 275/2006 Z.z.	o informačných systémoch verejnej správy v znení neskorších predpisov
Zákon č. 610/2003 Z.z.	o elektronických komunikáciách v znení neskorších predpisov
Zákon č. 215/2002 Z.z.	o elektronickej podpise v znení neskorších predpisov a prislúchajúce vyhlášky NBÚ
Výnos Ministerstva financií o štandardoch pre informačné systémy verejnej správy Slovenskej republiky č. 312/2010 Z.z.	o štandardoch pre informačné systémy verejnej správy
Zákon č. 122/2013 Z.z.	o ochrane osobných údajov
Zákon č. 215/2004 Z.z.	o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
Štandard STN ISO/IEC 27001	Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti
Štandard STN ISO/IEC 20000	Informačné technológie. Manažment služieb.
Zákon č. 45/2011 Z. z.	o kritickej infraštruktúre
Vyhláška Úradu na ochranu osobných údajov č. 164/2013 Z.z.	o rozsahu a dokumentácii bezpečnostných opatrení
Vyhláška NBÚ č. 336/2004	o fyzickej bezpečnosti a objektovej bezpečnosti v znení neskorších predpisov

DataCentrum v rámci existujúceho legislatívneho prostredia už v súčasnosti pôsobí ako nadrezortný poskytovateľ IT služieb pre organizácie verejnej správy. V zmysle cieľov štúdie sa adresuje interný rozvoj (kvantitatívny a kvalitatívny) DataCentra s cieľom poskytovať IT služby s vyššou pridanou hodnotou pre subjekty verejnej správy. Vychádzajúc z predpokladu, že existujúce pôsobenie DataCentra je v súlade s platnou legislatívou, je možné konštatovať, že neexistujú zásadné právne bariéry pre realizáciu daného projektového zámeru.

3.2 Biznis architektúra

3.2.1 Konsolidácia IKT pre organizácie štátnej správy

Správa IKT pre verejnú správu je riadená v rámci kompetencií jednotlivých rezortov, resp. subjektov verejnej správy. Na národnej úrovni momentálne neprebíha reálna aktivita (projekt), ktorej cieľom by bola konsolidácia IKT, čo spôsobuje, že väčšina subjektov štátnej správy rozvíja väčšie alebo menšie výpočtové strediská.

Na úrovni rezortu MF SR je zrejma snaha o vybudovanie zdieľaného dátového centra, ktorá už priniesla prvé výsledky. DataCentrum ako rozpočtová organizácia MF SR už v súčasnosti poskytuje služby aj pre iné rezorty a niektoré inštitúcie samosprávy.

DataCentrum aj MV SR majú v rámci svojho rozvoja ambíciu poskytovať IT služby na vyžiadanie orgánom verejnej správy v takom rozsahu, ktorá ich odbremení od starostlivosti o ich IT zdroje (nákup potrebných zariadení, pravidelný update SW a upgradu HW, SW aplikácií a pod.) a zároveň im umožní znížiť náklady na informačné a komunikačné technológie. Základom je prenesenie starostlivosti o IT prevádzku a infraštruktúru na DataCentrum (resp. MV SR) ako poskytovateľa komplexných služieb, aby sa efektívne využívali verejné financie.

3.2.2 Projekty PO1 OPIS

V súčasnosti sú ciele PO1 OPIS realizované formou samostatných projektov, pri ktorých nie sú vytvorené systémové predpoklady pre zdieľanie a konsolidáciu HW a SW infraštruktúry. Jednotliví žiadatelia majú vybudovanú rôznu úroveň IKT infraštruktúry od komplexných dátových centier so zabezpečením disaster recovery až po jednoduché data room spĺňajúce požiadavky podľa štandardu Uptime Institute na úrovni Tier I, resp. Tier II.

V zmysle koncepcie budovania ISVS podľa NKIVS a aj charakteru poskytovaných eGov služieb sa požaduje dostupnosťou systémov v rozsahu 24x7. Zabezpečenie takejto dostupnosti vyžaduje dátové centrá na úrovni Tier III vrátane záložných (disaster recovery) lokalít.

PO1 OPIS projekty primárne implementujú komplexné a jedinečné informačné systémy, ktoré vyžadujú integráciu na ostatné systémy ISVS.

3.2.3 Dátové centrá vo verejnej správe SR

V máji 2013 uskutočnilo Ministerstvo financií SR prieskum medzi jednotlivými organizáciami štátnej správy, z ktorého je možné zistiť prehľad v niektorých dôležitých oblastiach. Pre potreby tejto štúdie sú to:

- Kvantitatívny prehľad aktuálnej IKT infraštruktúry
- Prehľad potrieb IKT infraštruktúry na najbližších 24 mesiacov
- Aktuálne kapacitné možnosti organizácií vzhľadom na definované potreby

Z odpovedí 12 rezortov, ktoré sú k dispozícii vyplýva, že tieto rezorty majú momentálne inštalovaných 1644 rackov pre potreby prevádzky informačných systémov spolu v primárnych aj záložných lokalitách. V týchto rackoch je prevádzkovaných 3434 fyzických serverov, na ktorých je 2415 aplikácií/informačných systémov (systémy sa môžu opakovať, pokiaľ rezorty prevádzkujú ten istý systém). 1035 aplikácií označili zástupcovia rezortov ako kritické.

Je dôležité vyzdvihnúť, že len 3 rezorty uviedli, že prevádzka aplikácií/informačných systémov v ich rezorte je zabezpečená záložnými lokalitami.

Z dotazníkov je možné konštatovať, že približne tretina serverov je virtualizovaná, prevažne technológiami Hyper-V a VMWare pre x86 servery a príslušnými technológiami výrobcov pre platformy IBM, HP v prípade serverov vyššej triedy.

Na základe zozbieraných údajov sa javí, že štátna správa disponuje dostatočnou rezervou v ploche, elektrickom a chladiacom výkone. Po vyhodnotení ďalších dôležitých parametrov sú však zrejmé nasledovné skutočnosti (počty sú zámerne formulované len ilustračne, nakoľko odpovede v prieskume neboli dostatočne exaktné pre získanie presných agregovaných údajov):

- Redundancia elektrického napájania
 - Drvivá väčšina dátových sál neobsahuje redundanciu v elektrickom napájaní
- Redundancia UPS
 - Pre väčšinu dátových sál je uvedené v kolónke miera redundancie UPS len N alebo N/A prípadne je kolónka prázdna. Len u cca 30% je uvedená čiastočná redundancia UPS.
- Redundancia motor-generátora
 - Žiadne dátové centrum nie je vybavené redundantným motor generátorom, čo zodpovedá klasifikácia Tier I. Približne 60% dátových centier nie je vybavených motor-generátorom.

Z uvedeného vyplýva, že kvalita jestvujúcich dátových centier je maximálne v kategórii Tier I alebo nekvalifikovateľná. Posilnenie daných priestorov na kvalifikovateľný štandard by si vyžiadalo nadmerné úsilie a veľa finančných prostriedkov s negarantovaným výsledkom, nakoľko veľká väčšina DC je v priestoroch, kde nie je ani technicky a priestorovo možné vykonať posilnenie na akceptovateľný štandard.

3.2.4 Súčasné a predpokladané využitie infraštruktúry DataCentra pre iné rezorty

Vzhľadom na to, že DataCentrum je vnímané ako rezortné integrované dátové centrum (RIDC), primárny poskytovateľ konsolidovaných IT služieb pre rezort MF SR, ostatné rezorty a samosprávu ako aj ich podriadené organizácie, dochádza už v dnešnej dobe k integrácii vybraných informačných systémov do DataCentra. V súčasnosti DataCentrum poskytuje nasledovné služby pre iné rezorty (organizácie).

- Zabezpečenie prevádzky informačných systémov SAP Ministerstva životného prostredia a Ministerstva dopravy, výstavby a regionálneho rozvoja, Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky (MZVaEZ), Ministerstvo školstva Slovenskej republiky (MŠ) a Ministerstvo hospodárstva Slovenskej republiky (MH).
- Pre samosprávne kraje DataCentrum poskytuje prevádzku SAP portálu štátnej pokladnice (Košický, Nitriansky a Banskobystrický samosprávny kraj) a prevádzku účtovníctva samosprávneho kraja (Nitriansky a Banskobystrický samosprávny kraj). Zo strany MF SR je záujem postupne rozširovať služby prevádzky SAP portálu štátnej pokladnice a prevádzky účtovníctva a poskytovať ich všetkým samosprávnym krajom a ich podriadeným organizáciám - celkovo cca 900 organizácií.
- Rozpočtový informačný systém pre samosprávu (RIS.SAM) - v procese nasadzovania na všetky mestá a obce - približne 3 000 organizácií miest a obcí v SR
- Jednotné účtovníctvo štátu (JÚŠ) - sú v ňom zahrnuté všetky organizácie štátnej a verejnej správy

Národné centrum zdravotníckych informácií (NCZI – v pôsobnosti Ministerstva zdravotníctva SR) v súčasnosti hľadá partnera pre prevádzku svojich informačných systémov pre poskytovateľov zdravotníckej starostlivosti v Slovenskej republike. Uvažuje sa s využitím DataCentra.

3.3 Aplikačná a dátová architektúra

3.3.1 DataCentrum

Technická infraštruktúra DataCentra je zameraná na zabezpečenie služieb informačných systémov pre inštitúcie verejnej správy a služieb podpory prevádzky pre tieto IS. Primárna orientácia je na informačné systémy MF SR, ale prevádzkované sú aj informačné systémy iných ministerstiev a niektorých inštitúcií samosprávy. Druhou oblasťou sú informačné systémy samotného DataCentra, slúžiace napr. na podporu používateľov prevádzkovaných IS, testovanie ako aj ďalšie menšie informačné systémy. Ako jedny z významných je možné uviesť nasledovné informačné systémy:

- Rozpočtový informačný systém (RIS)
- Informačný systém Štátnej pokladnice (IS ŠP)
- Informačný systém jednotného účtovníctva štátu (JÚŠ),
- Záložný systém ARDAL (Agentúra pre riadenie dlhu a likvidity)

Informačné systémy Ministerstva financií Slovenskej republiky, Ministerstva životného prostredia Slovenskej republiky (MŽP); Ministerstva dopravy, výstavby a regionálneho rozvoja Slovenskej republiky (MDVRR), Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky (MZVaEZ), Ministerstva školstva Slovenskej republiky (MŠ) a Ministerstva hospodárstva Slovenskej republiky (MH):

- Rozpočtový IS pre samosprávu (RIS.SAM)

- Informačný systém Nitrianskeho (NSK) a Banskobystrického samosprávneho kraja (BBSK)
- Informačný systém štrukturálnych fondov (ITMS)
- Informačný systém účtovníctva fondov (ISUF)
- Centrálny elektronický priečinok (CEP)
- Register účtovných závierok (RÚZ)
- Register ponúkaného majetku štátu (www.ropk.sk)
- Systémy pre integračné a automatizované testovacie centrum (IATC)
- Skupina podporných systémov, medzi ktoré patrí napr. systém Call Centra, Service Desk, Centrum podpory používateľov (CPU) a Centrálny Monitoring Prevádzky (CMP)
- Portály rozpocet.sk, informatizacia.sk, registeruz.sk, ropk.sk

3.3.2 Ministerstvo vnútra SR

Informačné systémy a ich aplikácie v dátových centrách MVSR sú rozdelené do viacerých aplikačných domén (oblastí):

- Aplikačná doména pre poskytovanie elektronických služieb občanom a organizáciám,
- Aplikačná doména Agend štátu a Policajných informačných systémov,
- Aplikačná doména Národného Schengenského informačného systému.

V rámci týchto domén sú vytvorené produkčné a testovacie prostredia jednotlivých informačných systémov. Aplikačné domény obsahujú informačné systémy:

- Doména elektronických služieb :
 - IS eGovernment
- Doména Agendy štátu :
 - IS Regob a IS Správne Agendy a IS Dokladové agendy
 - Policajné IS MVSR (PIS MVSR)
- Doména Národný Schengenský informačný systém:
 - IS Schengen II

Informačné systémy obsahujú jednotlivé aplikácie, ktoré sa v danom čase nachádzajú v rôznych štádiách svojho životného cyklu (test, produkcia). Z pohľadu OPIS sú relevantné nasledovné informačné systémy:

- Informačné systémy v pokročilom štádiu implementácie
 - IS registra fyzických osôb - RFO
 - Elektronické služby matriky - CISMA

- Elektronické služby centrálnej ohlasovne - CO
 - Elektronická identifikačná karta - EID
 - Informačný systém Registra adries - RA
 - Elektronické služby národnej evidencie vozidiel - NEV
 - Elektronické služby pre osvedčenie o evidencii vozidla - eTP
 - Informačné systémy s pripravovanými projektmi
 - IS identifikátora fyzických osôb - IFO
 - El. Archív MV SR
 - Elektronické služby informačných systémov MVSR na úseku PZ policajného zboru
- Elektronické služby Živnostenského registra

Prístup k aplikáciám v jednotlivých aplikačných doménach je z prostredí:

- Intranet MVSR (MV-Net),
- Internet,
- Externé siete (napr. Govnet),
- EU net pre Schengen IS.

Prístup k aplikáciám je možný pre koncových používateľov cez grafické používateľské prostredie (GUI) alebo pre aplikácie cez Webové služby (Web Services).

Prístup k aplikáciám je oddelený a chránený prostredníctvom bezpečnej prístupovej zóny.

3.4 Infraštruktúra

Popis aktuálneho stavu infraštruktúry sa primárne orientuje na aktuálny stav dátových sál DataCentra a Ministerstva vnútra SR, nakoľko ide z pohľadu zámeru projektu o najrelevantnejšie subjekty.

3.4.1 DataCentrum

3.4.1.1 Dátová sála

Dátová sála PDC je umiestnená na 1. poschodí budovy DataCentra a má celkovú rozlohu 246,3 m². Technické prevedenie IT systémov na dátovej sále je primárne orientované na umiestnenie v dátových skriniach (stojanoch), s výnimkami ako napr. servery pre uzol prepojenia na EÚ (TAXAD) a systémami ktoré je možné z hľadiska veľkosti považovať za samostatné dátové stojany (napr. server Superdome, diskové polia a pod.). Interné dátové rozvody sú realizované prostredníctvom metalickej kabeláže kategórie 6 a viac a optickej kabeláže, využívanej primárne pre SAN infraštruktúru.

Celkovo sa naplnenie dátovej sály v súčasnosti pohybuje na úrovni cca 55 dátových stojanov, takmer všetky v prevedení 42U. Z tohto počtu je 51 dátových stojanov využitých pre IT systémy (servery, diskové polia, ...) a 4 pre pasívne a aktívne prvky interných dátových rozvodov (LAN, SAN). Väčšina dátových stojanov pre serverové systémy je obsadená na cca 80% až 90%.

V súčasnosti, pri počte 55 dátových rozvádzačov, sú priestory dátovej sály využité na cca 64% a je možné rátať s umiestnením ešte cca 31 nových dátových stojanov pre serverové systémy. Celkové naplnenie sály predstavuje cca 86 dátových stojanov.

V blízkej budúcnosti sa v dátovej sále predpokladá umiestnenie systémov Ministerstva zdravotníctva, čo predstavuje požiadavku na priestor cca 20 nových dátových stojanov.

Plánovaná je optimalizácia IT systémov, ktorej výsledkom má byť aj redukcia počtov fyzických serverov prostredníctvom konsolidácie a virtualizácie IT systémov.

3.4.1.2 Napájanie

Napájanie všetkých dátových stojanov je realizované z dvoch nezávislých vetiev, kde každá vetva má 1 samostatný elektrický rozvádzač, 1 UPS, 1 transformátor a napájanie z elektrickej rozvodnej siete, pričom výpadok jednej vetvy neovplyvní prevádzku systémov.

Primárne napájanie je zabezpečované prostredníctvom dvojice transformátorov (hlavný a záložný), každý s výkonom 630 kVA. Priamo v dátovej sále sa nachádzajú 2 rozvádzače s redundantným výkonom 490 kW, z ktorých sú vedené 2 redundantné vetvy napájacích rozvodov pre dátové stojany. Rozvádzač každej vetvy je zálohovaný pomocou UPS s výkonom 240kW, ktorá má dobu zálohovania cca 30 minút. Celkovo je napájanie zálohované ešte dieselgenerátorom CATERPILLAR s výkonom 700 kVA.

Aktuálna záťaž od inštalovaných IT systémov na dátovej sále je 115 kW a sumárny odber, vrátane klimatizačných zariadení, je 211 kW. To predstavuje v súčasnosti výkonovú rezervu o veľkosti 125 kW.

3.4.1.3 Klimatizácia

Chladenie dátovej sály je realizované prostredníctvom 6 klimatizačných skriň UNIFLAIR, s celkovým chladiacim výkonom cca 240 kW. Každá skriňa má dva chladiace okruhy s kondenzátormi umiestnenými na streche. Na zabezpečenie dostatočného chladiaceho výkonu bez ohrozenia prevádzky je akceptovaný výpadok 2 chladiacich skriň.

3.4.1.4 Protipožiarny systém

Dátová sála je vybavená EPS (elektronickou požiarnou signalizáciou) a automatickým hasiacim systémom. Informácie protipožiarného systému sú vyvedené aj do monitorovacieho systému dátovej sály APC InfraStruXure.

3.4.1.5 Monitorovacie systémy

Významným prvkom zabezpečenia chodu technologických systémov dátovej sály je monitorovací systém APC InfraStruXure, pomocou ktorého je možné včas identifikovať problémy v systémoch chladenia, napájania a ostatných podporných sústav. Monitorovací systém tiež umožňuje posielat' varovné maily a SMS na vybrané adresy.

3.4.1.6 Záložné dátové centrum

Pre časť informačných systémov prevádzkovaných v DataCentre je vytvorený aj záložný systém, ktorý je prevádzkovaný v záložnom dátovom centre formou housingu (umiestnenie vlastných systémov v priestoroch cudzieho dátového centra) – t.j technologická infraštruktúra je zabezpečovaná formou služby. Záložné dátové centrum sa nachádza v lokalite mimo Bratislavy.

3.4.1.7 Prehľad IKT infraštruktúry

Systémová infraštruktúra DataCentra obsahuje viac tried serverov:

- Najvyššia trieda – HP Integrity Superdome (HP Superdome SD 64)
 - informačné systémy na platforme SAP, UNIX platforma
- Stredná trieda – rad HP 9000, Unix platforma
- Nižšia trieda (x86 servery HP) – platforma Windows, Linux
 - Viaceré servery su virtualizované (VMWare)
 - Využívané pre bežné aplikácie a portály, prístupovú infraštruktúru (doménové servery, MS Active Directory, mail server, Citrix farma, VPN)

Infraštruktúra pre ukladanie dát obsahuje tiež niekoľko tried diskových polí SAN a páskové knižnice. SAN inraštruktúra je len lokálna (bez prepojenia do záložného dátového centra), všetky zariadenia sú do SAN siete prepojené minimálne duálnymi cestami.

Siete WAN komunikačnej infraštruktúry zabezpečujú sprístupnenie informačných systémov prevádzkovaných v DataCentre pre klientské organizácie a používateľov, prostredníctvom sietí označovaných ako Finnet a 5HQ.

- Finnet 1 – predstavuje VPN pre systémy KTI (komunikačno – technologická infraštruktúra), prostredníctvom ktorých DataCentrum poskytuje služby prístupu k aplikáciám pre rozsiahlu množinu organizácií štátnej správy, Štátnej pokladne a ich pobočiek,
- Finnet 2 – predstavuje VPN sieť pre Finančnú správu SR. Do tejto štruktúry patria aj existujúce siete Daňovej a Colnej správy, ktoré smerom na KTI využívajú existujúce prepojenie 5HQ pevnými linkami,
- Finnet 3 - vznikol po zavedení ServiceDesku pre Nitrianský samosprávny kraj. Tvorí ho 114 liniek, ktoré zabezpečujú komunikáciu medzi pracoviskami,
- Finnet 4 – zabezpečuje prepojenie miest , obcí a samospráv,

- Sieť 5HQ – sieť spájajúca vrcholové orgány rezortu - MF SR, FS SR a Štátna pokladnica / ARDAL.

Siete sú postavené na infraštruktúre siete ST-MPLS a ST-MEN a predstavujú navzájom oddelené VPN siete.

Vytvorené je tiež priame prepojenie do záložného DRC Tajov na úrovni LAN, ktoré je šifrované. Zriadené sú 2 fyzické prepojenia – jedno sa využíva pre zrkadlenie databáz, na úrovni prostriedkov Oracle a druhé pre synchronizáciu systémov Citrix. Ďalšie fyzické prepojenie je vytvorené do primárneho dátového centra ARDAL a je dedikované len pre systém ARDAL.

Monitoring systémov zabezpečujú dva systémy s logickým označením Konzola 1 a Konzola 2. Konzola 1 predstavuje starší systém určený na monitorovanie IS ŠP a ďalších kľúčových systémov (JUŠ, SAP,...). Monitorovací systém je postavený na produkte HP OVO (Open View Opeartion) a NNM (Network Node Manager). Vybrané udalosti sa posielajú do aplikácie HP Service Manager.

K dispozícii sú dva samostatné zálohovacie systémy, ktoré priamo súvisia s využitím páskových knižníc.

- Zálohovací systém pre internú sieť (interné systémy) – využíva jednu knižnicu MSL 6060. Riadenie zálohovania zabezpečuje aplikácia HP Data Protector.
- Samostatný zálohovací systém pre systémy ŠP a ostatné systémy. Využíva ostatné dve knižnice. Zálohovanie je riadené druhou aplikáciou HP Data Protector.

Pre podporu používateľov je využívaná aplikácia HP Service Manager. Používatelia prístupujú k aplikácii prostredníctvom WEB rozhrania. Do systému sú prenášané aj vybrané udalosti z monitorovacích systémov.

3.4.2 Ministerstvo vnútra SR

V dvoch dátových centrách MV SR (DC Timravy, DC Tajov) je zabezpečená produkčná a testovacia prevádzka informačných systémov MV SR. Architektúra a implementácia IT infraštruktúry umožňuje efektívne využitie zdrojov oboch Dátových centier (režim Aktívny/Aktívny) a schopnosť rýchlej obnovy po havarijnej situácii v jednom z dátových centier (HA&DR, High Availability, Disaster recovery). Aplikačné systémy, resp. aplikácie MV SR, ktoré sú prevádzkované v dvoch dátových centrách MV SR:

- DCA Timravy,
- DCB Tajov.

Základné architektonické technologické princípy riešenia sú:

- Model dátových centier “Aktívne – Aktívne“ so synchronnou replikáciou dát medzi dátovými centrami.
- Geografický klaster pre perzistentnú (databázovú) vrstvu medzi dátovými centrami,
- Zdieľaný klastrový súborový systém so synchronnou replikáciou dát medzi dátovými centrami,

- Manažment domény aplikačných serverov (WAS cells) v rámci dátového centra,
- Synchronná replikácia na úrovni diskových polí (MetroMirror) s implementáciou ConsistencyGroup,
- Global Site Balancing s DNS.

Každá aplikačná skupina využíva :

- dedikované technologické komponenty IT infraštruktúry,
- spoločné technologické komponenty IT infraštruktúry.

Každá aplikačná doména obsahuje okrem aplikácií aj dedikované infraštruktúrne technologické komponenty (konfigurácie).

Na zabezpečenie HA a DR riešenia je v geograficky vzdialenom dátovom centre DCB Tajov umiestnená výkonovo a architektonicky rovnocenná HW infraštruktúra, ktorá je schopná prevádzkovať produkčné systémy MV SR v plnej funkčnosti.

3.4.2.1 Dátová sála – primárne DC (Timravy)

DC Timravy bola vybudovaná v roku 2004. Od tohto času boli do sály postupne pridávané ďalšie systémy, kapacita sály je na hranici. Pridanie ďalších systémov už nie je možné.

Rozloha IT sály je cca 140m² a max. záťaž je dimenzovaná na cca 120kW. Súčasná obsadenosť a záťaž dosahuje kapacitné limity. Dátové centrum je dizajnované v štandarde Tier II s jednou vetvou napájania a priemernou štatistickou dostupnosťou 99,749%. Infraštruktúra kritických systémov neumožňuje odstávku alebo servis za prevádzky.

DC Timravy sa v aktuálnom čase vzhľadom na intenzívny rozvoj IKT v rezorte MV SR ukazuje ako kapacitne nedostatočné pre najkritickejšie systémy zo strednodobého a dlhodobého pohľadu z nasledovných dôvodov:

- Sálu už nie je možné priestorovo rozširovať, pričom sála je aktuálne využívaná na 100%
- V sále nie je možné ďalej rozširovať technológie chladenia, čo už v aktuálnom stave predstavuje v letných mesiacoch problém pre dostatočné chladenie existujúcej IKT infraštruktúry
- Obdobne sú obmedzené možnosti navýšenia kapacity elektrického napájania
- Sála neumožňuje odstávku alebo servis za prevádzky (v zmysle požiadavky Tier III)
- Sála sa nachádza v záplavovej oblasti rieky Hron
- Sála sa nachádza v obytnej štvrti v tesnej blízkosti obytných objektov, čo nie je optimálne riešenie najmä z dôvodu bezpečnosti a hlučnosti prevádzky podporných technológií (chladenie, motor generátor)

3.4.2.2 Napájanie

Zálohované napájanie je na úrovni Tier II s jednou vetvou napájania. Zálohovanie je riešené s použitím UPS v redundancii N+1 a motor-generátora. Infraštruktúra napájania neumožňuje zásah / odstavenie alebo servisovanie za prevádzky bez výpadku IT systémov.

3.4.2.3 Klimatizácia

Klimatizácia je riešená v 5 split systémami v redundancii N+1 rozmiestnenými v 2 technologických miestnostiach.

3.4.2.4 Protipožiarny systém

DC Sála je vybavená automatickým hasiacim systémom na báze vodnej hmly napojeným na systém EPS a systém skorej detekcie požiaru Firetracer.

3.4.2.5 Dátová sála – záložné DC (Tajov)

DC Tajov bolo pôvodne budované ako záložné stredisko. V súčasnosti je toto dátové centrum využívané v produkčnom režime.

3.4.2.6 Monitorovanie

Systémový monitoring: na serveri pmon je nainštalovaný monitorovací systém pre servre Power, ktorý poskytuje aktuálne a aj historické údaje o využití/zaťažení zdrojov serverov.

Pre Databázový monitoring dbmon je realizovaná infraštruktúra zdieľaného FS.

3.5 Bezpečnostná analýza

V rámci elektronizácie verejnej správy dochádza k nárastu vytvárania a spracúvania aj informácií strategického charakteru v elektronickej forme. Aktuálny stav zabezpečenia týchto informácií a s nimi spojených služieb jednotlivých IS nepokrýva všetky riziká. Verejná správa sa zvyšovaním elektronizácie stále častejšie bude stávať obeťou útokov organizovaných i neorganizovaných hackerských skupín. Nedostatočné zabezpečenie IS, nedoriešené procesy riadenia a udržiavania informačnej bezpečnosti a nezáujem o problematiku tieto riziká zvyšujú. Závislosť elektronickej verejnej správy na funkčných a bezpečných službách IS bude časom narastať a bude si vyžadovať aj vyššie zabezpečenie týchto IS a údajov, ktoré sú v nich spracúvané.

Dôsledky nedostatočného riešenia informačnej bezpečnosti môžu byť veľmi široké a závažné, s celospoločenským negatívnym dopadom, napr.:

- únik citlivých finančných údajov strategického charakteru v dôsledku hackerského prieniku, alebo počítačovej infiltrácie s konečnými dôsledkami pre štát,
- oneskorenia pri strategických aktivitách inštitúcií verejnej správy v dôsledku nepripravenosti na úmyselne zapríčinené výpadky IS,

- neoprávnené zverejnenie citlivých údajov o občanoch,
- únik internej elektronickej korešpondencie zamestnancov obsahujúcej citlivé údaje a mnohé ďalšie.

Ako už bolo konštatované aj v iných štúdiách uskutočniteľnosti vo verejnej správe sú väčšinou prednostne nasadené informačné systémy pre podporu agend, ktorých výkon a spracovanie je priamo určené legislatívnymi normami, pričom využívanie IS v špecializovaných okruhoch ako aj ich centralizácia sa môže významne líšiť. Architektúra prevádzkovaných IS pritom nie vždy umožňuje komplexné riadenie informačnej bezpečnosti a v prípade kritických systémov zabezpečenie vysokej dostupnosti.

Aktuálna dekompozícia IS verejnej správy zvyšuje aj nároky a náklady na riešenie informačnej bezpečnosti. Služby súvisiace s riadením informačnej bezpečnosti ako aj samostatný výkon sa väčšinou deje pre každý IS autonómne a v rámci inštitúcie verejnej správy, ktorá za daný IS zodpovedá.

3.5.1 Legislatívne východiská

Legislatívne a štandardizačné prvky obsahujú a agregujú široké spektrum požiadaviek informačnej bezpečnosti a pre potreby realizácie projektov PO 1 OPIS musia byť správne interpretované. Ide hlavne o nasledujúce zákony, normy a strategické dokumenty:

- Národná koncepcia informatizácie verejnej správy,
- Národná stratégia pre informačnú bezpečnosť v SR a úlohy Akčného plánu na roky 2008 až 2013,
- Zákon č.275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. 9. júna 2010 o štandardoch

pre informačné systémy verejnej správy,

- Oznámenie Komisie Európskemu parlamentu o „Ochrane Európy pred rozsiahlymi kybernetickými útokmi a narušeniami, zvyšovanie pripravenosti, bezpečnosti a odolnosti“ z roku 2009,
- Zákon č. 122/2013 Z.z. o ochrane osobných údajov,
- Vyhláška Úradu na ochranu osobných údajov č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení,
- Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov,
- Štandard STN ISO/IEC 27001 Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti,

- Štandard STN ISO/IEC 27002 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti,
- Štandard STN ISO/IEC 27005 Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti
- Bezpečnostná politika IS rezortu MF SR,
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre.

4 Popis cieľového stavu

4.1 Legislatívna analýza

Projekty budovania dátových centier a ich spoločného využívania viacerými organizáciami verejnej správy už sú realizované a funkčné, čo poukazuje na priaznivý stav legislatívy v tejto oblasti. Nepredpokladáme teda nutnosť významných zmien ako predpokladu pre realizáciu projektu.

Zmeny môžu vyplynúť zo snahy prevádzkovať v predmetnom dátovom centre špecifické systémy rezortov, pri ktorých je nakladanie s údajmi resp. informačnými systémami upravené špecifickou legislatívou.

Pre dosiahnutie čo najvyššej efektivity pri budovaní informačných systémov verejnej správy a k nim prislúchajúcej infraštruktúry však štúdia odporúča prijatie legislatívneho rámca, ktorý zadefinuje povinnosť využívať Dátové centrum ako platformu pre prevádzku informačných systémov s definovanými vlastnosťami (napr. požadovaná dostupnosť, citlivosť spracovávaných údajov a podobne). Takýto legislatívny akt by mal byť minimálne na úrovni uznesenia vlády, ktoré by zaviazalo všetkých ministrov, resp. organizácie v ich pôsobnosti.

4.2 Analýza požiadaviek a potrieb stakeholderov

Potreby v oblasti základnej IKT infraštruktúry typicky nie sú priamymi potrebami, ale potrebami vyvolanými z vyšších úrovní, t.j. v hierarchii od efektívnej správy vecí verejných a potreby efektívnej interakcie verejnosti s verejnou správou, cez elektronické služby, informačné systémy a následne HW a SW platformy, na ktorých sa prevádzkujú ide o potreby na najnižšom stupni. Zároveň ale ide o priestor, kde je možné najviac a relatívne najjednoduchšie optimalizovať využitie zdrojov či už koncentráciou do väčších a efektívnejších dátových sál, zdieľaním IKT infraštruktúry, príslušného technického vybavenia a v neposlednom rade aj obslužného personálu, až po virtualizáciu serverov a zdieľanie zdrojov na čo najvyššej úrovni.

V tejto kapitole sa štúdia nebude venovať opakovaniu potreby zavedenia cloudu verejnej správy, ktorý je v dokumente viac krát popisovaný, ale zameria sa na konkrétne potreby vyplývajúce z už spomínaného prieskumu Ministerstva financií SR medzi jednotlivými rezortmi.

Z prieskumu vyplýva, že jednotlivé rezorty plánujú v priebehu 24 mesiacov osadiť 350 rackov za účelom prevádzky dodatočných 673 fyzických serverov na ktorých bude prevádzkovaných 247 kritických aplikácií. Ide o pomerne netypický pomer počtu rackov a fyzických serverov (veľmi nízky priemerný počet serverov na rack), ktorý je možné aspoň čiastočne vysvetliť situáciou na Ministerstve kultúry SR, kde je vzhľadom na charakter informačných systémov možné predpokladať veľké nároky na dátové úložiská a nie výpočtovú kapacitu. Ministerstvo kultúry SR z počtu 350 rackov pripravuje až 104, pričom plánuje osadiť 107 serverov.

Okrem x86 serverov je plánované aj obstaranie serverov na platforme IBM Power7 (Ministerstvo vnútra SR). V prípadoch, kde rezort odpovedá na otázku týkajúcu sa plánovanej

virtualizácie serverov je odpoveď kladná – približne na úrovni 80%. Virtualizačné technológie pre x86 servery sú plánované podľa platforiem Hyper-V a VMWare.

Zo spomínanej potreby 673 serverov (počet serverov bol vybraný ako najreprezentatívnejšia metrika spomedzi dodaných údajov vzhľadom na vyššie spomenuté diskrepancie v počtoch serverov oproti rackom) vyplýva pri približnej obsadenosti 10 až 12 serverov na rack potreba približne 60 rackov. Na dodatočnú infraštruktúru (sieťové komponenty, diskové úložiská, ...) je potrebných rádovo 20% priestoru pre servery, teda cca 12 rackov. Tieto čísla vychádzajú z plánu na 24 mesiacov, pričom vo výhľade minimálne 5 rokov je potrebné počítať s dvojnásobkom tejto kapacity aj pri zohľadnení optimalizácií vďaka efektívnej správe a využitiu virtualizácie. Predpokladaná potrebná kapacita dátového centra je teda približne pre 150 rackov, čo značí minimálne 400m² plochy dátovej sály v závislosti od zónovania, veľkosti rackov a technických dispozícií sály (sál). Pre väčšinu systémov je potrebné prevádzkovať aj minimálne jednu záložnú lokalitu s porovnateľnými IKT požiadavkami, takže je potrebné v úhrne počítať s dvojnásobkom tejto plochy, teda 800 m² rozdelenými do viacerých geograficky oddelených dátových sál.

4.2.1 Rozvoj komunikačno-technickej infraštruktúry ISVS na centrálnej úrovni

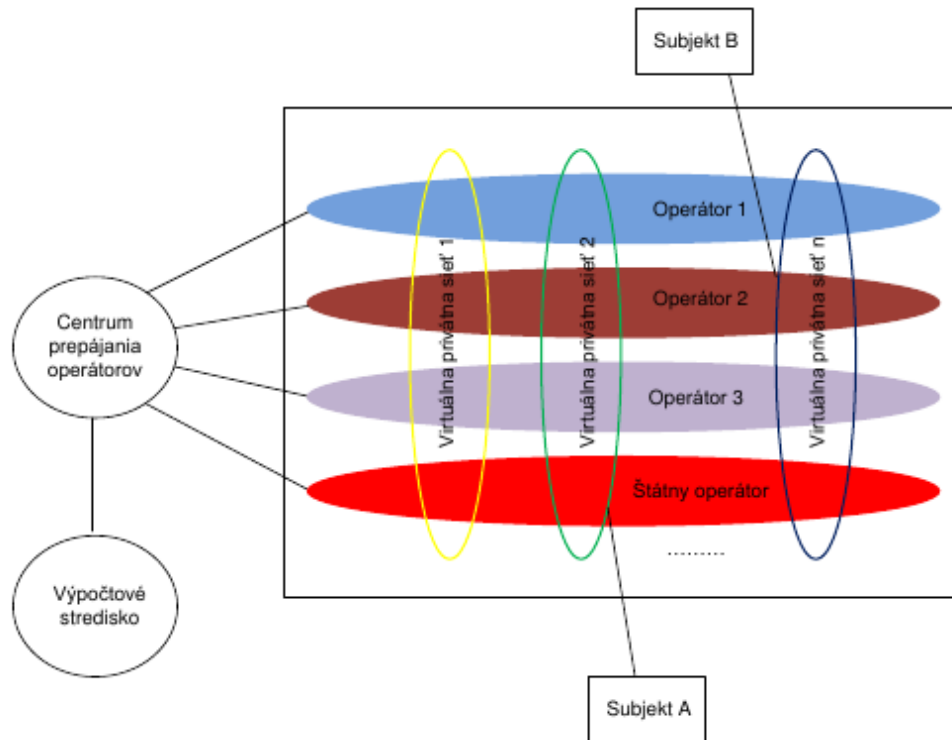
V rámci PO1 OPIS bola v roku 2009 vypracovaná „Štúdia uskutočniteľnosti prioritnej osi č. 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS zameraných na rozvoj komunikačno-technologickej infraštruktúry IS verejnej správy na centrálnej úrovni“ (ďalej aj Štúdia RKTÍ). Primárnym cieľom Štúdie RKTÍ bolo navrhnutie efektívneho a účinného postupu implementácie projektov pre zabezpečenie komunikačno-technologickej infraštruktúry informačných systémov verejnej správy v súlade s celkovou architektúrou integrovaného informačného systému verejnej správy.

Štúdia RKTÍ ako cieľové riešenie rozpracovala alternatívu, ktorej charakteristika je z pohľadu komunikačnej a technologickej infraštruktúry popísaná v nasledujúcich bodoch:

Komunikačná infraštruktúra :

- Použije sa obmedzený počet operátorov. S operátormi bude uzavretá rámcová zmluva na dobu určitú. Po jej uplynutí bude opätovne vyhodnocovaná kvalifikácia.
- Zodpovednosť za vzájomné prepojenie operátorov, tak aby bolo možné prepojenie jednotlivých VPN štátnej správy, je na strane operátorov.
- Samospráva sa bude pripájať do VPN štátnej správy pre oblasť prenesených kompetencií.

- Ministerstvo financií SR bude držiteľom Kontrolnej a koordinačnej kompetencie s praktickým dosahom na kvalifikáciu operátorov, podmienky poskytovania služieb (SLA)



Obrázok 1 Schéma konceptu prepojenia operátorov

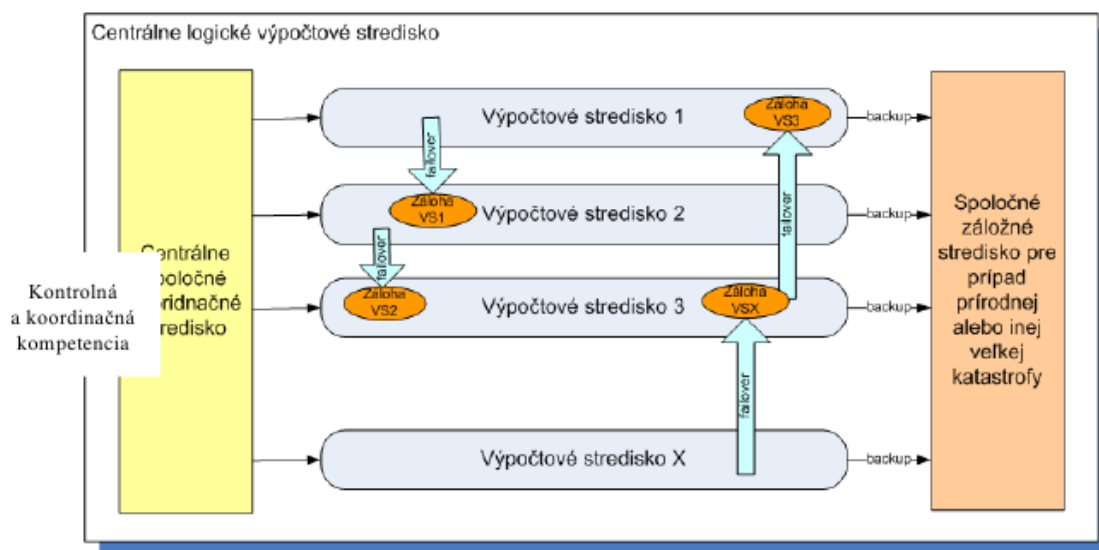
Z pohľadu technologickej infraštruktúry Štúdia RKTÍ navrhla vybudovanie centrálného logického výpočtového strediska, ktoré predstavuje logickú úroveň fyzických dátových centier. Skladá sa zo samostatných fyzických dátových a spoločného záložného strediska pre prípad prírodnej alebo inej veľkej katastrofy. Štúdia RKTÍ predpokladala kvalifikáciu 7 dátových centier, ktoré prináležia nasledovným povinným osobám: Ministerstvo financií SR, Úrad vlády SR, Ministerstvo vnútra SR, Sociálna poisťovňa, Úrad geodézie, kartografie a katastra SR, Ministerstvo zdravotníctva SR (NCZI), Štatistický úrad SR.

Koordináciu činnosti jednotlivých fyzických dátových centier je zabezpečená Kontrolnou a koordinačnou kompetenciou, ktorá:

- Koordinuje a metodicky usmerňuje chod samostatných výpočtových stredísk
- Obsahuje centrálny monitoring chodu služieb jednotlivých výpočtových stredísk
- Nezasahuje priamo do chodu jednotlivých výpočtových stredísk

Ostatné výpočtové centrá sú hostované kvalifikovanými dátovými centrami. Časť dátových centier (nekvalifikovaných) bude „prežívať“ naďalej. Od programu OPIS sa očakávala finančná motivácia tých, ktorí podporia implementáciou navrhovaný model, reprezentovaný kvalifikovanými dátovými centrami. Tak bude dochádzať k tesnejšej forme navrhovanej

centralizácie.



Obrázok 2 Centrálne výpočtové stredisko

Štúdia RKTÍ zároveň identifikovala nasledovné kľúčové riziká spojené s budovaním centralizovanej IKT infraštruktúry:

- Organizačné riziká a problémy:
 - neochota poskytovať služby DC iným rezortom
 - neochota umiestniť spravované zdroje do kvalifikovaných dátových centier
 - nebudú vytvorené organizačné a personálne predpoklady na fungovanie kvalifikovaných dátových centier
- Technologické riziká a problémy
 - technologické obmedzenia migrácie aplikácií do kvalifikovaných dátových centier
 - nekompatibilita systémov z dôvodu veľkej diverzifikácie platforiem
 - nemožnosť virtualizácie
 - nedostatočné kapacity kvalifikovaných dátových centier
- Legislatívne riziká a problémy
 - nebudú vytvorené legislatívne predpoklady na vytvorenie Centrálneho logického dátového centra štátu
 - legislatívny proces vytvorenia podmienok na centralizáciu bude trvať dlho

4.3 Popis navrhovaného riešenia

4.3.1 Biznis architektúra

Hlavné ciele a požiadavky z pohľadu biznis aspektov je možné zhrnúť do nasledovných bodov:

- Skonsolidovať IKT infraštruktúru naprieč organizáciami tam, kde je to možné, vhodné a výhodné
- Vybudovať základné technické predpoklady (dátovú sálu) pre budúce poskytovanie služieb privátneho cloudu verejnej správy
- Zabezpečiť spoločnú prevádzku vybraných IS organizácií verejnej správy – primárne ide o jednoduchšie systémy a štandardné systémy, ktoré nevyžadujú komplexné špecifické know-how
- Pre Ministerstvo vnútra SR riešiť preťaženosť aktuálneho DC Timravy aj s ohľadom na implementované/plánované informačné systémy

Biznis aspekty riešenia sú popísané v nasledovných kapitolách nasledovnými spôsobmi

- Vízia rozvoja dátových centier vo verejnej správe
- Princípy a požiadavky na riešenie
- Katalóg služieb poskytovaných budúcim dátovým centrom
- Analýza procesov súvisiacich s prevádzkou budúceho dátového centra a poskytovaním služieb

4.3.1.1 *Vízia rozvoja dátových centier vo verejnej správe*

Z analýzy existujúceho stavu dátových centier uvedenej v predošlých kapitolách je zrejma veľká rozdrobenosť a decentralizácia existujúcich dátových centier vo verejnej správe. Tento stav z dlhodobého hľadiska nie je možné považovať za efektívny a je preto prirodzené, že Ministerstvo financií SR ako inštitúcia zodpovedná za informatizáciu má ambíciu tento stav riešiť.

Realizovanie a prevádzkovanie budúceho centralizovaného logického dátového centra štátu je komplexná úloha, ktorá pre úspešné zrealizovanie vyžaduje dôsledné pokrytie mnohých aspektov, pričom za najdôležitejšie považujeme:

- Organizácia – pre budovanie a rozvoj je nevyhnutné disponovať tímom odborníkov na strane verejnej správy ktorí majú dostatočné skúsenosti s dátovými centrami a riadením dodávateľov, v spolupráci s ktorými budú schopní zrealizovať požadovaný cieľ
- Finančné – konsolidovaná základná infraštruktúra zodpovedajúca vysokým štandardom vyžaduje nemalé investície jednak na prvotnú realizáciu ale následne aj na dlhodobú prevádzku. Prevádzkovateľ musí mať zabezpečené dostatočné prostriedky pre celý životný cyklus dátového centra.

- Technické – stavať nové logické dátové centrum (niekoľko fyzických) na zelenej lúke je investícia presahujúca možnosti financovania a nesmeruje k efektívnemu využitiu už existujúcich dátových centier, preto je dôležité vychádzať už z aktuálneho technického stavu a pri realizácii cieľového dátového centra využiť existujúce dátové centrá a technológie.
- Legislatívne – pre efektívny tlak na konsolidáciu základnej infraštruktúry je vhodné adekvátne nastaviť aj legislatívne prostredie, aby podporovalo ďalšiu konsolidáciu a smerovanie investícií do znovupoužiteľnej spoločnej infraštruktúry s možnosťami flexibilnej alokácie zdrojov a kontrolovateľného rozširovania konsolidovanej infraštruktúry. Legislatíva a kontrola na druhej strane musí zabrániť neefektívnym investíciám do samostatnej infraštruktúry tam, kde to nie je dostatočne odôvodnené napr. dodatočnými bezpečnostnými požiadavkami alebo iným závažným argumentom.

Z vyhodnotenia aktuálneho stavu dátových centier, plánu rozvoja infraštruktúry jednotlivých rezortov a vyššie-uvedených aspektov sa pre riešenie budúceho dátového centra ponúkajú 2 organizácie:

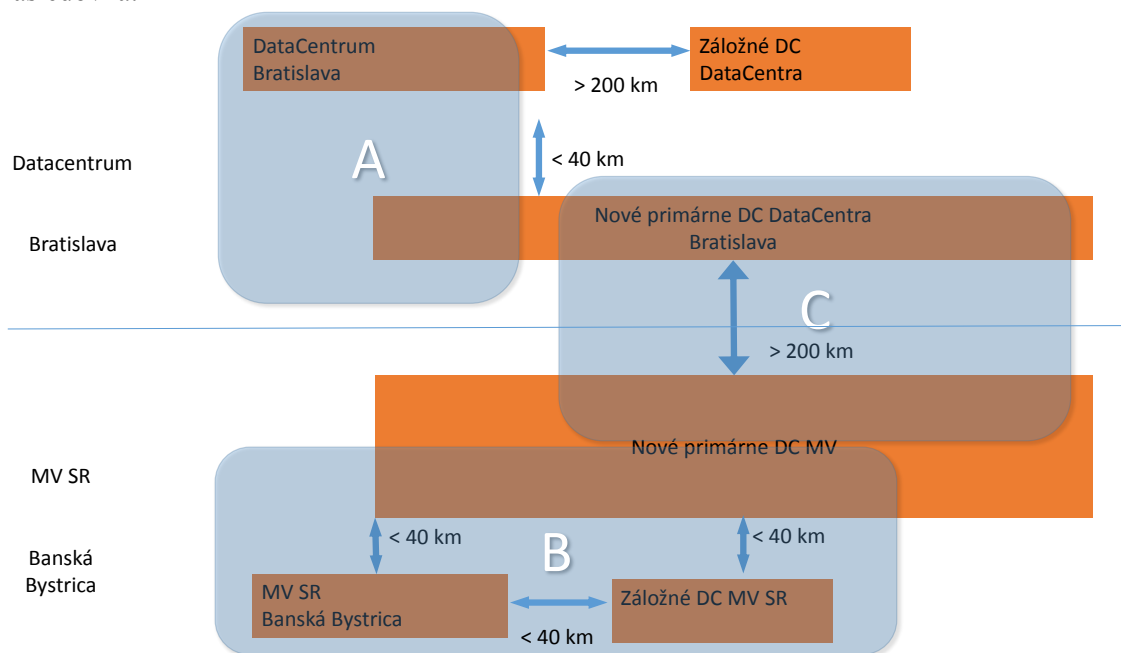
- Ministerstvo financií SR, resp. jeho rozpočtová organizácia DataCentrum
 - Disponuje 6 dátovými sálami s úhrnnou IT plochou vyše 600 m² a realizuje vo svojej gescii niekoľko významných systémov eGovernmentu, pričom už v čase tvorby tejto štúdie prevádzkuje systémy iných rezortov. Má teda organizačné a technické predpoklady a je zodpovedné za legislatívu v oblasti IKT na Slovensku.
- Ministerstvo vnútra SR
 - Prevádzkuje 2 dátové centrá (primárne dátové centrum s rozlohou približne 140 m², záložné dátové centrum riešené formou nájmu), zodpovedá za správu kľúčových referenčných registrov, prevádzkuje kritické ISVS a okrem uvedených predpokladov navyše prevádzkuje svoju infraštruktúru v geograficky vzdialených lokalitách (Banská Bystrica a okolie), čo pri efektívnom prepojení s dátovými centrami v Bratislave môže významne zvýšiť bezpečnosť riešenia logického dátového centra štátu.

Koncepcný návrh budúceho dátového centra vychádza okrem vyššie uvedeného aj z nasledovných skutočností a predpokladov:

- Celková predpokladaná potreba infraštruktúry vo verejnej správe je v úhrne 400m² (viď 4.2 Analýza požiadaviek a potrieb stakeholderov).
- Aktuálna zaplnenosť súčasných dátových centier DataCentra a MV SR je vyše 80% (64% v DataCentre a 100% v MV SR).
- Väčšina ISVS vyžaduje pre efektívne podporovanie procesov štátu dostupnosť zodpovedajúcu dátovým centrom na úrovni Tier III
- Len niekoľko systémov je aktuálne vysoko kritických a teda vyžadujúcich architektúru, ktorá úplne minimalizuje výpadky, na čo okrem iného potrebuje nasadenie v dvoch súčasných aktívnych uzloch (active-active). Ide primárne o niektoré komponenty systému eHealth, vybrané systémy Ministerstva vnútra SR (napr. Schengenský informačný systém – SIS, niektoré budované základné komponenty eGovernmentu ako napr. RFO a RPO) a niekoľko ďalších špecializovaných systémov. Preto nie je nevyhnutné budovať nové fyzické dátové centrá vo vzdialenosti do 40 km typicky vyžadovanej pre synchronne zapisovanie do databáz a súborových systémov

- Pre zabezpečenie požadovanej dostupnosti väčšiny ISVS je potrebné počítať s nasadením v dvoch lokalitách, pričom sekundárna lokalita slúži na prevádzkovanie systému v prípade nedostupnosti primárnej lokality, či už z dôvodu údržby alebo nepredvídateľnej udalosti (porucha, nehoda, živelná katastrofa). Tieto lokality by mali byť dostatočne geograficky vzdialené, aby najmä živelná udalosť v jednej lokalite neovplyvnila prevádzku v druhej.

Na základe vyššie uvedeného by cieľová architektúra logického dátového centra štátu mala byť nasledovná:



Obrázok 3 Cieľová architektúra logického dátového centra štátu

V schéme sú znázornené:

- V hornej časti dátové centrá v pôsobnosti DataCentra (geograficky Bratislava a okolie)
 - 2 existujúce využívané dátové centrá DataCentra
 - Plánované nové väčšie dátové centrum DataCentra
- V dolnej časti dátové centrá Ministerstva vnútra SR (geograficky Banská Bystrica a okolie)
 - Plánované nové dátové centrum MV SR
 - 2 existujúce dátové centrá MV SR

Okrem dátových centier a orientačné ohraničenia dĺžky ich sieťových prepojení sú znázornené aj zóny v rámci ktorých budú cieľovo prevádzkované ISVS

- A – zóna primárne pre ISVS vyžadujúce architektúru active-active, ktoré sú prevádzkované DataCentrom (momentálne ide primárne o komponenty systému eHealth)

- B – zóna primárne pre ISVS vyžadujúce architektúru active-active, ktoré sú prevádzkované MV SR (napr. Schengenský systém na ochranu štátnej hranice Slovenskej republiky s Ukrajinou)
- C – cieľová zóna pre poskytovanie služieb privátneho cloudu verejnej správy. Všetky nové ISVS vo verejnej správe implementované v čase, keď budú známe špecifikácie a podmienky tohto cloudu, by mali smerovať do tohto priestoru.

Okrem scenárov prevádzky systémov v zónach A, B a C predpokladá dátové centrum aj nasledovné situácie:

- Umiestnenie záložnej infraštruktúry (či už ide o sekundárny alebo tretí – disaster recovery - uzol) pre ISVS organizácie verejnej správy, ktorej primárny uzol si táto organizácia prevádzkuje na svojej infraštruktúre. V tomto prípade je možné použiť voľnú kapacitu ľubovoľného dátového centra so zohľadnením iných požiadaviek (napr. geografická vzdialenosť, požadovaná kapacita, ...)
- Prevádzka ISVS už dnes prevádzkovaných v existujúcich dátových centrách DataCentra a MV SR do ukončenia ich životného cyklu tam, kde nemá opodstatnenie investícia do migrácie do cloudu.

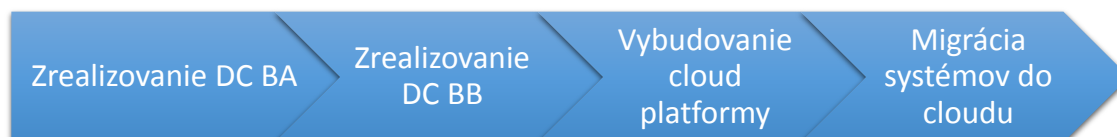
Stav, ku ktorému by logické dátové centrum štátu malo dlhodobo smerovať je presun všetkých prevádzkovaných systémov do cloudu. Vzhľadom na predpokladaný rast počtu informačných systémov a teda aj IKT zdrojov potrebných na ich prevádzkovanie sa nedá predpokladať, že tento cieľový cloud bude prevádzkovaný len v dvoch lokalitách. Cloud technológie ale sú pripravené na nasadenie v zložitejších ako dvoj-lokalitných topológiách a preto sa očakáva po premigrovaní informačných systémov z pôvodných datacentier do cloudu, resp. ukončení ich životného cyklu, pripájať aj infraštruktúru pôvodných dátových centier do cloudu. Vo veľkej miere bude ale predpokladom generačná výmena IKT, resp. obnova základnej infraštruktúry dátových sál tak, aby bola možná bezproblémová a bezriziková integrácia.

Pre prevádzku privátneho cloudu verejnej správy bude potrebné zdefinovať okrem technických aspektov aj maticu zodpovedností. Rozloženie medzi 2 zodpovedné organizácie prináša výhodu konsenzu a spoločného postupu, ktorý by mal zabezpečiť dlhodobo udržateľné fungovanie, avšak prináša aj komplikáciu v podobe delenia zodpovedností. Riešení sa ponúka niekoľko:

- Vybudovanie 2 nezávislých cloud platforiem na spoločnej infraštruktúre – toto riešenie môže rozšíriť možnosti pre prevádzkované systémy a zaviesť flexibilitu rozširujúcu množinu systémov, ktoré bude možné prevádzkovať v cieľovom cloudu.
- Rozdelenie kompetencií medzi DataCentrom a MV SR v rámci prevádzky jednej cloud platformy – najkomplikovanejší variant vzhľadom na potrebu a náročnosť komunikácie a vzájomného zladzovania a jednoznačnosti zodpovedností za prevádzkované systémy.
- Poverenie jednej organizácie, resp. jej zriadenie za účelom správy cloudu – najmenej pravdepodobná cesta vzhľadom na zbytočné trieštenie personálnych zdrojov a administratívnu náročnosť takéhoto úkonu pri vytváraní novej organizácie, resp. nižšiu akceptáciu a silu pri presadzovaní riešenia, komplikovaný vzťah k základnej infraštruktúre (ktorá je rozdelená medzi MV SR a DataCentrum) pri poverení len jednej z týchto dvoch organizácií správou cloudu.

- Vzhľadom na uvedené výhody a nevýhody a možnosť zavedenia (aj keď dočasnej) „súťaže“ medzi dvoma platformami sa pri dostatočnej efektívite vynakladania verejných zdrojov javí ako najúčinnnejšia možnosť budovania dvoch nezávislých cloud platforiem.

Rámcový plán aktivít smerujúcich k vybudovaniu načrtnutého dátového centra je nasledovný:



Obrázok 4Rámcový plán aktivít

Zrealizovanie dátového centra DataCentra – tento krok bol ako prvý zvolený vzhľadom na nutnosť riešenia problémov s infraštruktúrnou kapacitou pre systémy ISVS. Zrealizovanie dátovej sály v okolí Bratislavy ponúka okrem výstavby aj relatívne širokú škálu existujúcich priestorov, ktoré vyhovujú požiadavkám a bolo by možné ich obstarat’.

Zrealizovanie dátového centra MV SR – druhý krok, ktorý môže prebiehať aj paralelne s prvým. V okolí Banskej Bystrice sa predpokladá adaptácia existujúceho objektu na dátovú sálu vzhľadom na veľmi malé možnosti obstarania existujúcich vyhovujúcich priestorov, ale aj vzhľadom na fakt, že Ministerstvo vnútra disponuje nehnuteľnosťami potenciálne vhodnými na adaptáciu na dátové sály. Tento krok bude vzhľadom na predpokladané stavebné práce zrejme bude trvať dlhšie ako dátové centrum v okolí Bratislavy.

Vybudovanie cloud platformy – obsahuje okrem výberu vhodného konceptu pre cloud a vybavenia sál vhodným IKT aj prípravu procesov a organizácie (nábor a vyškolenie personálu). Táto etapa môže tie prebiehať paralelne s predošlými krokmi, keďže príprava je rozsiahla a pilotné projekty je možné prevádzkovať aj na menšej infraštruktúre.

Migrácia systémov do cloudu – finálna etapa transformácie vyžadujúca detailné naplánovanie, otestovanie a komunikáciu pre zabezpečenie plynulého prechodu do cieľovej architektúry.

4.3.1.2 Princípy konsolidácie základnej infraštruktúry a požiadavky na riešenie

Centrálne služby poskytované Dátovým centrom vytvárajú priestor pre konsolidáciu požiadaviek na IKT infraštruktúru jednotlivých projektov PO1 OPIS a iných IS verejnej správy a z toho vyplývajúcu úsporu nákladov na obstaranie a prevádzku informačných systémov verejnej správy. Možné úspory spojené s využitím služieb Dátového centra vyplývajú z:

- **Konsolidácia infraštruktúry** – konsolidácia infraštruktúry umožňuje zdieľanie a efektívne využitie dostupných zdrojov. V spojení s virtualizáciou a šandardizáciou vytvára podmienky pre také riadenie kapacít, ktoré umožňuje pokryť plánované požiadavky a minimalizuje objem nevyužitých zdrojov.
- **Úspora nákladov na energie** – náklady na energie predstavujú v súčasnosti 15-20% nákladov na celkové vlastníctvo (TCO). Veľké dátové centrá sú schopné nakupovať energie za výhodnejšie sadzby. Vďaka konsolidovanej infraštruktúre sú schopné dynamicky optimalizovať záťaž a využitie zdrojov a tým efektívne riadiť aktuálnu spotrebu energie.

- Úspora nákladov na pracovnú silu – prostredie veľkých dátových centier umožňuje automatizáciu opakovaných úloh manažmentu IKT prostredia aj v takých prípadoch, ktoré by boli pre menšie dátové centrá finančne neefektívne. Masívna automatizácia následne umožňuje pracovníkom dátového centra obslužiť väčšie množstvo IKT prvkov a sústrediť sa na úlohy s vyššou pridanou hodnotou.
- Kúpna sila – prevádzkovatelia veľkých dátových centier nakupujú hardvér, softvér a služby vo veľkom čo im dáva predpoklady na získanie výhodnejšej ceny ako v prípade menších nákupcov.

Riešenie dátového centra musí na najvyššej úrovni spĺňať okrem vyššie uvedených konsolidovaných požiadaviek jednotlivých organizácií nasledovné principiálne požiadavky:

- Efektivita
- Bezpečnosť
- Dostupnosť
- Modularita
- Rozšíriteľnosť
- Interoperabilita
- Virtualizácia
- Merateľnosť
- Zohľadnenie najlepších praktík

4.3.1.3 Princípy návrhu riešenia

Efektivita

Dátové centrum musí byť budované so zreteľom na dosiahnutie maximálnej efektivity pri využití zdrojov a minimalizácii prevádzkových nákladov pri dodržaní požadovaných parametrov poskytovaných služieb. Princíp efektivity musí byť adresovaný vo všetkých oblastiach Dátového centra. Dodržanie tohto princípu umožní v konečnom dôsledku naplniť jeden z primárnych cieľov riešenia, ktorým je znižovanie nákladov na informačné systémy verejnej správy.

Bezpečnosť

Bezpečnosť je prioritou pri zanedbaní ktorej môže dôjsť k vážnemu ohrozeniu aktív zákazníka a jeho partnerov a môže mať kľúčový dopad na celý sektor. Na úrovni dátového centra je potrebné venovať primárnu pozornosť nasledovným oblastiam informačnej bezpečnosti:

- Fyzická bezpečnosť
- Bezpečnosť prostredia

- Bezpečnosť informačných a komunikačných technológií

Analýza a návrh naplnenia požiadaviek jednotlivých oblastí informačnej bezpečnosti vrátane určenia spôsobov dosiahnutia trvalo udržateľnej adekvátnej úrovne informačnej bezpečnosti musí byť neoddeliteľnou súčasťou implementácie dátového centra vo forme príslušného bezpečnostného projektu.

Bezpečnosť rovnako ako modularita má zásadný vplyv aj na dostupnosť. Jednou z oblastí bezpečnosti je aj ochrana.

Dostupnosť

Zabezpečenie požadovanej dostupnosti je základnou prioritou riešenia. Dostupnosť je pritom chápaná vo vzťahu ku koncovému odberateľovi služieb čo vytvára vysoké nároky na všetky komponenty infraštruktúry, ktoré sa podieľajú na poskytovaní služieb dátového centra:

- podpornú technológiu
- komunikačnú technológiu
- informačnú technológiu

Zabezpečenie požadovanej úrovne dostupnosti bude dosiahnuté prostredníctvom redundantných komponentov a fail-over mechanizmov.

Modularita

Modularita umožňuje zefektívniť prevádzku, prípadné technické zásahy, obnovu technicky alebo morálne zastaraných technických prostriedkov alebo softvéru. Prevádzkovateľovi zjednodušuje dohľad a manažment. Pri hľadaní chýb umožňuje ich izoláciu a tým ich jednoduchšie a rýchlejšie odhalenie a odstránenie. Tým má zásadný vplyv aj na dostupnosť.

Rozšíriteľnosť

Rozšíriteľnosť v zmysle kapacít a ponúkaných služieb je ďalším kľúčovým princípom. Riešenie Dátového centra je potrebné navrhnuť tak, aby umožňovalo naplniť súčasné ako aj očakávané budúce požiadavky. V rámci rozšíriteľnosti je potrebné optimálne riešiť konflikt medzi nákladmi, predpokladanou dobou prevádzky DC a krátkym životným cyklom IKT technológií. Rovnako je potrebné brať do úvahy, že požiadavky na kapacitu dátových centier a služieb s nimi spojených budú počas prevádzky prirodzene rásť. Kľúčovým je navrhnuť optimálny počiatočný stav a stanoviť rozvojový plán tak, aby bolo možné zabezpečiť potrebnú kapacitu včas a finančne efektívne.

Princíp rozšíriteľnosti adresuje aj požiadavku na pružnosť a elasticitu výpočtových kapacít z pohľadu odberateľa služieb. Riešenie Dátového centra je potrebné navrhnuť tak, aby umožňovalo rýchlu a jednoduchú zmenu kapacít.

Interoperabilita

Interoperabilita na úrovni infraštruktúry a technických celkov IT je dosiahnutá využitím štandardov a musí byť riešená v rámci vypracovania detailnej architektúry a konfigurácie systémov. Táto úroveň zabezpečuje technické fungovanie infraštruktúry.

Virtualizácia

Virtualizácia infraštruktúry podporuje rýchle nasadenie, vysokú flexibilitu a zvyšovanie efektivity nákladov na správu a údržbu. Umožňuje vytvárať a prevádzkovať služby privátneho cloudu (IaaS) s využitím vlastnej fyzickej infraštruktúry.

Merateľnosť

Všetky poskytované služby musia byť monitorované a získané dáta priebežne vyhodnocované. Meranie je dôležité pre všetky typy služieb nakoľko poskytuje komplexný prehľad o fungovaní jednotlivých služieb, aplikácií, ich výpočtových potrebách a o aktuálnom využití dostupného výkonu a kapacít. Merateľnosť je kľúčovým princípom, ktorý vytvára nutné podmienky pre samotné riadenie poskytovaných služieb.

Zohľadnenie najlepších praktík

Pri návrhu dátového centra sa vychádza zo štandardu Uptime Institute, resp. štandardov pre telekomunikačnú infraštruktúru dátových centier ANSI/TIA-942 a ANSI/NECA/BICSI-002, ktoré definujú referenčný model (rámec požiadaviek a najlepších praktík) pre návrh a implementáciu dátových centier. Štandard organizácie Uptime Institute definuje 4 kategórie dátových centier:

- Tier I. Základné – 99,67% dostupnosť
- Tier II. S redundantnými komponentmi – 99,75% dostupnosť
- Tier III. S možnosťou výkonu údržby bez nutnosti odstavenia IKT – 99,98% dostupnosť
- Tier IV. Odolné voči jednej chybe – 99,99% dostupnosť

Uvedená kategorizácia je podrobnejšie popísaná v ďalších častiach tejto kapitoly.

V oblasti riadenia prevádzky sú zohľadnené štandardy ISO 20000 a framework ITIL V3, ktorý okrem iného definuje procesy a funkcie pre riadenie prevádzkových činností smerujúcich k efektívnej dodávke poskytovaných služieb.

V oblasti riadenia informačnej bezpečnosti sa vychádza zo štandardu ISO 27001 a ISO 27002.

4.3.1.4 Služby dátového centra

Služby poskytované dátovým centrom sú na základe svojho charakteru rozdelené do troch kategórií:

- primárne – základné služby, ktoré poskytujú požadovanú infraštruktúru a zabezpečenie prevádzkových činností
- podporné – poskytujú podporu riadenia prevádzky
- telekomunikačné – služby zabezpečujúce komunikáciu v rámci verejnej správy a využívanie služieb Internetu

Pre všetky služby dátového centra budú definované:

- Charakteristika – popis základných parametrov služby udržiavaný v rámci katalógu služieb
- SLA - určuje zmluvné podmienky pre dodávku služby
- Nákladový model – definuje náklady na poskytovanie služby
- Model spoplatnenia – definuje spôsob spoplatnenia

Služby uvádzané nižšie je potrebné chápať ako pohľad na aktuálne možnosti typicky poskytované dátovými centrami a cloud platformami. Výsledná množina služieb bude upravená vzhľadom na možnosti ich poskytovania či už z pohľadu technického, finančného, legislatívneho alebo organizačného a samozrejme vzhľadom na záujem o využívanie jednotlivých typov služieb. Zároveň predpokladáme postupné zavádzanie týchto služieb a prípadnú evolúciu v pridávaní resp. odoberaní služieb, ich zoskupovania do balíkov a úprave SLA podľa potreby.

Služby sú navyše rozdelené do dvoch etáp, v ktorých je možné ich implementovať:

- Prvá etapa – služby poskytované v novej dátovej sále
- Druhá etapa (nie je predmetom aktuálneho projektu) – budúce služby cloudu verejnej správy

Prvá etapa – služby poskytované v novej dátovej sále

Primárne služby - Poskytnutie priestoru (housing)

Poskytnutie priestoru dátového centra určeného pre osadenie vlastnej technickej infraštruktúry odberateľa. Priestor môže byť poskytnutý vo forme:

- dátového rozvádzača (racku)
- časti dátového rozvádzača
- základnej plochy dátového centra

Okrem samotného priestoru je súčasťou poskytovanej služby:

- redundantné elektrické napájanie vrátane záložného zdroja UPS
- redundantné chladenie
- služby:
 - bezpečnostných systémov PSN, SKV a PTV

- systémov požiarnej ochrany EPS, SDP a SHZ
- sieťová konektivita na chrbticovú sieť dátového centra

Primárne služby - Poskytnutie SAN infraštruktúry vrátane diskového priestoru

Poskytnutie dohodnutej kapacity SAN infraštruktúry a dátového úložiska na diskovom poli dohodnutej triedy. Služba môže byť bližšie špecifikovaná

- kapacitou
- šírkou pásma
- latenciou

Primárne služby - Poskytnutie zálohovacej infraštruktúry

Poskytnutie dohodnutej triedy a kapacity zálohovacej infraštruktúry pre infraštruktúru umiestnenú v dátovom centre.

Okrem samotného priestoru môže byť súčasťou poskytovanej služby:

- Bezpečný priestor pre skladovanie záloh (trezor)

Podporné služby - Dohľad

Služba predstavuje súbor aktivít, ktoré sú vykonávané s cieľom priebežného sledovania stavu odoberaných služieb vrátane technických komponentov, ktoré sa podieľajú na ich poskytovaní. Dohľad centralizuje zber a spracovanie „systémových“ udalostí nad IKT infraštruktúrou a „bezpečnostných“ udalostí vyvolaných narušením definovaných bezpečnostných politík. Súčasťou služby je:

- analýza a riešenie udalostí v súlade s dohodnutými podmienkami
- výkon nápravných opatrení po zachytení známej udalosti
- poskytovanie informácií o stave IKT
- notifikácia určených osôb zákazníka o definovaných udalostiach
- generovanie a poskytovanie reportov

Telekomunikačné služby - Pripojenie do internetu

Služba zabezpečuje redundantný širokopásmový prístup do Internetu ako doplnok k ostatným službám.

Telekomunikačné služby - Pripojenie do rezortných sietí

Zabezpečuje vysokorýchlostné pripojenie do rezortných WAN sietí. Súčasťou služby môže byť:

- vytváranie virtuálnych sietí
- zabezpečenie VPN prístupov

Druhá etapa – budúce služby cloudu verejnej správy

Po zavedení cloudu verejnej správy môžu byť služby dátového centra rozšírené o ďalšie služby umožňujúce poskytovanie infraštruktúry a služieb hlbšej granularity s väčšou flexibilitou a možnosťou dynamickej správy pridelených zdrojov:

- Primárne služby - Poskytnutie servera (IaaS)
 - Poskytovanie serverov a súvisiacej technickej infraštruktúry určenej pre prevádzku informačných systémov odberateľa. Poskytovanie systémových zdrojov bude zabezpečené prostredníctvom virtualizačnej infraštruktúry, ktorá umožňuje flexibilnú a dynamickú alokáciu zdrojov, zvyšuje finančnú efektivitu a znižuje požiadavky na správu a prevádzkovú podporu.
- Primárne služby - Poskytnutie dátového úložiska (IaaS)
 - Poskytovanie storage kapacít pre uloženie dát prevádzkovaných IS odberateľa.
- Primárne služby - Prevádzka informačného systému (SaaS)
 - Poskytuje komplexnú starostlivosť o prevádzku informačného systému objednávateľa v prostredí dátového centra.
- Podporné služby - Zabezpečenie trvalej kontinuity
 - Rozširuje službu „Prevádzka informačného systému“ o zabezpečenie kontinuity definovanej IKT infraštruktúry a príslušného aplikačného vybavenia aj v prípade katastrofickej udalosti.
- Podporné služby - Aplikačná podpora
 - Služba zabezpečuje priebežnú podporu aplikačného programového vybavenia počas celého životného cyklu od identifikácie a špecifikácie požiadaviek až po podporu testovania, nasadenia a údržby.
- Podporné služby - Používateľská podpora
 - Podpora koncových používateľov informačných systémov na úrovni evidencie a riešenia servisných hlásení (incidentov a požiadaviek) a metodologickej podpory pri používaní informačného systému
- Podporné služby - Zálohovanie a obnova
 - Služba zabezpečuje ochranu systémových a aplikačných dát pred stratou a poškodením prostredníctvom riadeného zálohovania a následnej obnovy.

4.3.1.5 Procesná analýza

Poskytovanie centrálnych služieb dátového centra je komplexná a náročná úloha, ktorá vyžaduje nasadenie procesov pre riadenie odberateľských (zákazníckych) vzťahov, procesov pre plánovanie, zavedenie a prevádzku poskytovaných služieb a podporných procesov pre riadenie internej organizácie.

Procesná analýza má za cieľ identifikovať základné procesy, ktorých implementácia je nutným predpokladom pre efektívne poskytovanie služieb dátového centra pri zabezpečení takej úrovne služieb, ktorá je požadovaná jej jednotlivými odberateľmi.

Procesy pre riadenie prevádzky budú postavené na štandardoch ISO 20000 a frameworku ITIL V3, ktorý okrem iného definuje procesy a funkcie pre riadenie prevádzkových činností smerujúcich k efektívnej dodávke poskytovaných služieb v rozsahu:

- Manažment udalostí
- Spracovanie požiadaviek
- Manažment incidentov
- Manažment problémov
- Manažment prístupov
- Service desk
- Technický manažment
- Manažment aplikácií
- Manažment IT prevádzky

Procesy pre správu poskytovaných IT služieb budú pre zvýšenie prehľadnosti rozdelené na základe životného cyklu riadenia IT služieb do nasledovných oblastí:

- Primárne procesy pre správu IT služieb
 - plánovanie
 - dizajn
 - zavedenie
 - prevádzka
- Zákaznícky orientované procesy
 - Manažment akvizícií
 - Aktivácia služby
 - Starostlivosť o zákazníka
- Podporné procesy

- Riadenie ľudských zdrojov
- Finančný manažment
- Obstarávanie
- Stratégia
- Právne a regulácia
- Bezpečnosť a riadenie rizík

4.3.1.6 Rozvoj služieb dátového centra

V rámci rozvoja služieb Dátového centra je prirodzeným krokom migrácia smerom ku cloud computingu, ktorý je spoločnosťou NIST (National Institute of Standards and Technology) definovaný ako model IT služieb, umožňujúci všadeprítomný, pohodlný, resp. na požiadanie možný sieťový prístup k zdieľaným oblastiam dynamicky konfigurovateľných výpočtových zdrojov, ktoré môžu byť rýchlo nasadzované a uvoľňované s minimálnymi nárokmi na jej manažment alebo vzájomnú súčinnosť s poskytovateľom tejto služby. K základným charakteristikám cloud computingu patrí:

- Samoobslužnosť – služby si môžu používatelia sami zriadiť, nakonfigurovať a používať.
- Prístup odkiaľkoľvek – služby sú dostupné prostredníctvom štandardného internetu cez širokú paletu klientských zariadení.
- Zdieľanie zdrojov – výpočtové zdroje sú zdieľané viacerými používateľmi bez ohľadu na to, kde sú umiestnené.
- Pružnosť – elasticita, ktorá umožňuje používateľom rýchlo upraviť (škálovať) kapacitu zdrojov podľa aktuálnej potreby.
- Meranie – používateľ platí len za to čo spotrebuje.

Distribučný model cloud computingu definuje tri základné formy poskytovaných služieb:

- Infraštruktúra ako služba (IaaS) – predstavuje poskytovanie virtualizovanej infraštruktúry. Zákazník používa a ovláda základné výpočtové zdroje. Má možnosť riadiť operačné systémy, dátové úložiská, nasadené aplikácie či sieťové komponenty infraštruktúry ale nie je umožnené ovládať/riadiť základnú cloud infraštruktúru, ktorá poskytuje všetky potrebné výpočtové zdroje pre užívateľské prostredie.
- Platforma ako služba (PaaS) – poskytuje komplexnú hardwarovú platformu, teda zariadenia a služby potrebné pre podporu úplného životného cyklu budovania aplikácií vrátane možnosti návrhu, vývoja, testovania a nasadenia. Používateľ ovláda (riadi) aplikácie, ktoré sú spustené v tomto prostredí (a má aj možnosť riadiť niektorú funkcionálnu hostujúceho prostredia), neriadi (nemá možnosť spravovať) operačné systémy, hardwarovú a sieťovú infraštruktúru, na ktorej sú aplikácie prevádzkované. Pre poskytovanie takejto miery abstrakcie je potrebné nasadiť služby pre vývoj a beh aplikácií, workload manažment, riadenie životného cyklu a manažment dát.

- Softvér ako služba (SaaS) – znamená poskytovanie aplikácií vo forme služieb. Používateľ nemusí, resp. nemá možnosť spravovať aplikáciu, platformu ani infraštruktúru.

Z pohľadu Dátového centra ako poskytovateľa služieb, ktorého zákazníkmi budú organizácie verejnej správy predpokladáme nasadenie cloud computingu formou privátneho cloudu. Služby budú poskytované iba pre konkrétne organizácie (len organizácie verejnej správy, nie široká verejnosť a podnikatelia) a poskytovaná infraštruktúra bude vytvorená vo virtuálnom prostredí vybraných dátových centier verejnej správy v rámci ich uzavretej infraštruktúry. Pri privátnom cloudu akýkoľvek IT zdroj rozprestretý naprieč organizáciami a je dynamicky doručovaný jednotlivým organizáciám podľa ich požiadaviek čo umožňuje dosiahnuť oveľa väčšiu efektivitu v poskytovaní týchto zdrojov. Pre odberateľov IT služieb by sa mali zdroje cloud computingu zdať neobmedzené. Preto je podmienkou pre dlhodobu efektívne fungovanie prostredia dobré kapacitné plánovanie, bez ktorého môže dôjsť k veľkému prebytku alebo nedostatku zdrojov. Z tohto pohľadu je privátny cloud náchylnejší na chyby v plánovaní, ktoré nie je možné vzájomne eliminovať medzi väčším počtom odberateľov. Na druhej strane však privátny cloud umožňuje lepšie zabezpečenie bezpečnosti, lepšie riadenie komunikácie, lepšie riadenie SLA a pod..

V porovnaní s poskytovaním služieb v rámci virtualizovanej infraštruktúry je prechod na privátny cloud rozšírením o:

- Automatizáciu procesov a samoobslužné rozhranie, ktoré umožňuje zriadenie služby na požiadanie.
- Vysokú automatizáciu v zmysle riadenia zdrojov, ktorá obsahuje všetko od infraštruktúry, middleware až po procesný manažment.
- Manažment prostredia s cieľom kontinuálneho zvyšovania efektívnosti prostredia.
- Sofistikované bezpečnostné a riadiace schopnosti, ktoré sú špecificky navrhnuté na základe požiadaviek organizácie.
- Priebežné riadenie úrovne služieb na základe aktuálnych požiadaviek organizácie.

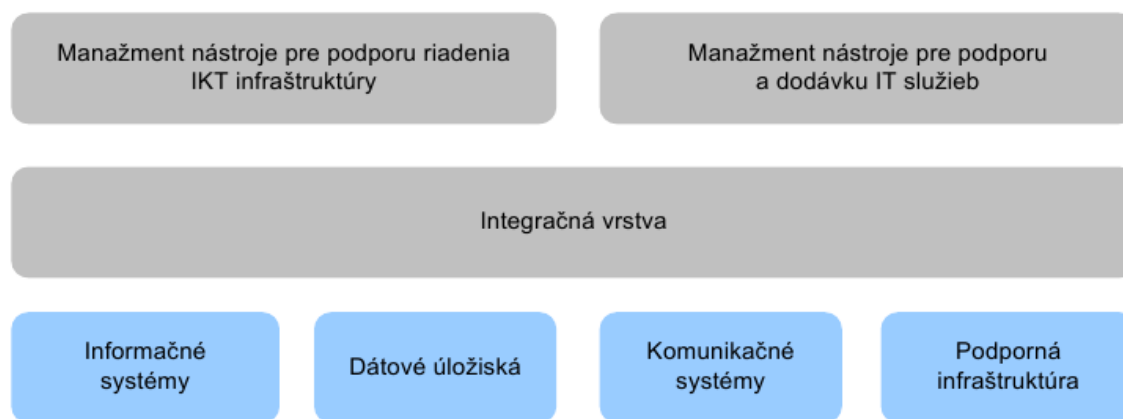
Komplexný prechod na poskytovanie služieb formou cloud computingu vyžaduje vyššiu mieru konsolidácie a štandardizácie ISVS, ktorá bude technologicky a organizačne náročná. Pred zahájením samotnej migrácie na cloud computing bude potrebné:

- analyzovať a špecifikovať očakávané ciele cloudu
- identifikovať služby
- dôkladne zvážiť predpokladané scenáre využitia
- posúdiť a ohodnotiť architektonické a technické obmedzenia aplikácií
- identifikovať a definovať legislatívne požiadavky
- identifikovať požiadavky na uloženie a ochranu údajov
- pripraviť stratégiu migrácie na cloud computing

Z pohľadu poskytovania služieb infraštruktúry (IaaS) dátového centra, je možné začať uplatňovať princípy cloud computingu takmer okamžite, pričom práve infraštruktúra resp. jej virtualizácia v Government Private Cloud-e a presun existujúcich aplikácií do tohto prostredia môže položiť základ na komplexný prechod ISVS.

4.3.2 Aplikačná a dátová architektúra

Vo fáze realizovania cieľového dátového centra je nevyhnutné okrem zabezpečenia technologickej infraštruktúry aj vybudovanie a integrácie manažment nástrojov pre podporu riadenia a dodávky IT služieb.



Obrázok 5 Logická architektúra

Integračná vrstva zabezpečuje výmenu dát, udalostí a transakcií medzi jednotlivými komponentmi IKT infraštruktúry a manažment nástrojmi. Zároveň vykonáva extrakciu dát z lokálnych dátových úložísk manažment nástrojov, ich transformáciu a uloženie do dátového skladu.

Manažment nástrojov pre podporu riadenia IKT infraštruktúry je zameraný na zabezpečenie požadovanej dostupnosti, kvality a flexibility technologickej, dátovej, komunikačnej, telekomunikačnej a informačnej infraštruktúry.

Manažment IKT a TI infraštruktúry napomáha výkonnosti a efektivite pri samotnej prevádzke a správe infraštruktúry tak, že umožňuje:

- riadiť zmeny komunikačnej a informačnej infraštruktúry tak, aby sa minimalizovali zdroje potrebné na elimináciu negatívnych následkov po implementácii zmien.
- monitorovať služby poskytované IKT a TI infraštruktúrou a analyzovať trendy tak, aby bolo možné v čo najkratšom čase a s minimálnym úsilím odstrániť identifikované problémy.

- predvídať a predchádzať problémom s výkonnosťou, kapacitou a dostupnosťou vrátane iniciovania nápravných aktivít.
- porozumieť celkovej infraštruktúre tým, že eviduje všetky komponenty a ich vzájomné väzby
- identifikovať nové technológie, ktoré umožňujú znižovať náklady, zvyšovať úroveň služieb a inovovať existujúce riešenia a procesy.
- plánovať rozvoj a údržbu IKT a TI tak aby bol vykonávaný v súlade s požiadavkami používateľov

Doména manažment nástrojov pre podporu riadenia IKT infraštruktúry zastrešuje tieto oblasti:

- monitorovanie a riadenie udalostí
- manažment podpornej technologickej infraštruktúry
- manažment telekomunikačnej infraštruktúry
- manažment dátových úložísk (pamäťových priestorov)
- manažment serverov
- manažment virtualizačného prostredia
- manažment databáz
- manažment výkonnosti a záťaže
- distribúciu softvéru
- inventarizácia hardvéru a softvéru
- automatizácia prevádzkových činností
- manažment licencií

Manažment nástroje pre podporu a dodávku IT služieb poskytujú služby “centra technickej kvality” pri návrhu, plánovaní a prevádzke IT služieb. Nepretržite monitorujú kvalitu infraštruktúry, služieb, vykonávajú analýzu a interpretáciu dát z manažment nástrojov a poskytujú vstupy pre proces návrhu a plánovania zmien v IKT infraštruktúre a IT službách.

Doména manažment nástrojov pre podporu a dodávku IT služieb zahŕňa:

- konfiguračnú databázu a manažment konfigurácie
- znalostnú databázu
- Service Desk a manažment incidentov
- manažment IT zmien
- katalóg IT služieb a manažment IT služieb
- riadenie dostupnosti IT služieb
- riadenie kontinuity IT služieb

Vo všeobecnosti sa manažment nástroje dajú rozdeliť do dvoch kategórií:

- platformové riešenia (suite)
- špecializované produkty

Variant A: Platformové riešenia

Platformové riešenia sa snažia pokrývať väčšinu aktivít spojených s manažmentom IKT infraštruktúry. Ponúkajú predpripravenú integráciu jednotlivých komponentov riešenia. Sú súčasťou širšieho portfólia produktov a nástrojov čím zvyšujú pravdepodobnosť toho, že dokážu v rámci tej istej platformy naplniť aj budúce užívateľské požiadavky.

Poskytujú globálne riadenie politík, unifikovaný rámec pre kód a objekty, jednotnú, resp. integrovanú používateľskú konzolu a podobný prístup k používateľskému rozhraniu čím zjednodušujú a zrýchľujú zaškolenie personálu a prijatie nástroja ako takého.

Sledujú „best practice“ v danom odvetví a ponúkajú implementáciu s predkonfigurovanými parametrami, resp. nástroje a techniky pre rýchle zavedenie a prispôbenie riešenia aktuálnemu prevádzkovému prostrediu.

Ponúkajú širokú podporu výrobcov hardvéru a softvéru, protokolov, technológií a metód. Sledujú vývojové trendy a priebežne rozširujú a dopĺňajú svoje portfólio podporovaných technológií. Taktiež ponúkajú platformovú nezávislosť z pohľadu inštalácie samotného riešenia.

Poskytujú rozsiahle API na štandardných technológiách (JAVA, web services, CORBA, ...), ktoré umožňuje integráciu manažment nástrojov tretích strán, externých dátových zdrojov a existujúcich informačných systémov.

Riešenia sú určené pre rozsiahle IKT prostredia s nepretržitou prevádzkou a tak majú už pri dizajne a vývoji natívne zabudované požiadavky na škálovateľnosť a vysokú dostupnosť. Samotná prevádzka je obvykle zabezpečená na dedikovaných zdrojoch (server, databáza, aplikačný server a pod.), ktoré sú oddelené od ostatných informačných systémov.

Nezanedbateľná je výhoda podpory celého riešenia jedným dodávateľom, ktorá zjednodušuje zmluvné vzťahy medzi organizáciou a dodávateľom, zjednodušuje údržbu a správu riešenia z pohľadu interných zdrojov a zvyšuje efektivitu komunikácie a riešenie problémov na tretej úrovni podpory.

Nevýhodou platformového riešenia je jeho komplexita, ktorá spôsobuje nárast požiadaviek na správu a údržbu spojenú s nevyhnutným personálnym zabezpečením.

Ďalšou negatívnou črtou centrálnych platforiem je nezladený a dlho trvajúci vývoj jednotlivých komponentov spôsobený priebežnými fúziami na trhu IT spoločností, ktoré si následne vynúti proces konvergenzie a integrácie novo nadobudnutých produktov do spoločnej platformy.

Variant B: Špecializované riešenia

Požiadavky manažmentu IKT infraštruktúry je možné pokryť špecializovanými, čiastkovými nástrojmi, ktoré sú zamerané na riešenie partikulárnych oblastí a častí IKT infraštruktúry.

Výhodou tohto prístupu je rádovo nižšia komplexita v porovnaní s platformovým riešením, ktorá umožňuje rýchle nasadenie a jednoduchšiu údržbu. Obvykle nevyžaduje ďalšie personálne kapacity na správu a údržbu. Špecializované riešenia zároveň pokrývajú aj oblasti, ktoré sú mimo záujmu veľkých platformových riešení či už z dôvodu malej zákazníckej bázy, nízkeho záujmu o danú funkcionálnosť, príliš hlbokú špecializáciu a pod.

4.3.3 Infraštruktúra

4.3.3.1 Metodológia a praktiky

Pri definovaní technických požiadaviek boli zohľadnené nasledovné zdroje:

- DC štandardy
- Lokálne normy a legislatíva
- Požiadavky výrobcov HW na prevádzkové podmienky IT

DC štandardy

Medzinárodné štandardy a metodológia pre budovanie infraštruktúry pre vysoko dostupné DC sú nasledovné:

- The Uptime Institute (Tier I – IV)
- TIA-942 - Telecommunications Infrastructure Standards for Data Center (Tier 1 – 4)
- ANSI/BICSI 002-2011 (Class F0 – F4)

Pre účely definovania požiadaviek na požadované DC bol použitý štandard podľa The Uptime Institute a vybrané požiadavky podľa TIA-942.

Pre definovanie požiadaviek na DC tieto neboli aplikované, nakoľko sa jedná o obdobné požiadavky ako TIA-942.

V ďalšom texte sú uvedené základné požiadavky na DC a ich porovnanie s príslušným štandardom.

The Uptime Institute

Štandardy definované The Uptime Institute sú všeobecne uznávané pre kritické riešenia vyžadujúce nepretržitú a spoľahlivú prevádzku. Definujú objektívne parametre pre porovnanie návrhov lokalít z hľadiska spoľahlivosti a dostupnosti. Stanovujú 4 kategórie (Tier I - IV) s parametrami na základe ktorých je možné zaradiť riešenie do príslušnej kategórie. Pre jednotlivé Tier definuje požadované:

- redundancie aktívnych komponentov
 - distribučné cesty
- systémov elektrického napájania a chladenia.

Na základe tejto klasifikácie ďalej stanovuje možnosti priebežnej servisovateľnosti a odolnosti týchto technológií a ich odolnosti voči jednej chybe.

Tabuľka 3 Tier požiadavky podľa The Uptime Institute

Položka	Tier I	Tier II	Tier III	Tier IV
Aktívne komponenty pre podporu IT záťaže	N	N+1	N + 1	N aj v prípade akejkoľvek poruchy
Distribučné cesty	1	1	1 aktívna a 1 náhradná	2 súčasne aktívne
Priebežná servisovateľnosť	Nie	Nie	Áno	Áno
Odolnosť voči jednej chybe)	Nie	Nie	Nie	Áno
Zónovanie	Nie	Nie	Nie	Áno
Nepretržité chladenie	Nie	Nie	Nie	Áno

Tabuľka 4 Vybrané typické parametre podľa The Uptime Institute podľa Tier

Položka	Tier I	Tier II	Tier III	Tier IV
Typ budovy	v nájme	v nájme	samostatná	samostatná
Najväčší výkon na rack (typicky)	<1kW	1-2kW	> 3kW	>4kW
Výška zdvojenej podlahy	30 cm	45 cm	75 – 90 cm	75 - 106 cm
Nosnosť podlahy	415kg/m2	490kg/m2	730 kg/m2	730+ kg/m2
Plánované servisné odstávky	2 krát ročne po 12 hodín	2 roky po 12 hodín	nie je nutné	nie je nutné
Dostupnosť vyplývajúca z prerušení prevádzky spôsobených lokalitou	99,67%	99,75%	99,98%	99,99%
Ročné prerušenie prevádzky	28,8 hodín	22 hodín	1,6 hodiny	0,8 hodiny

Tier I

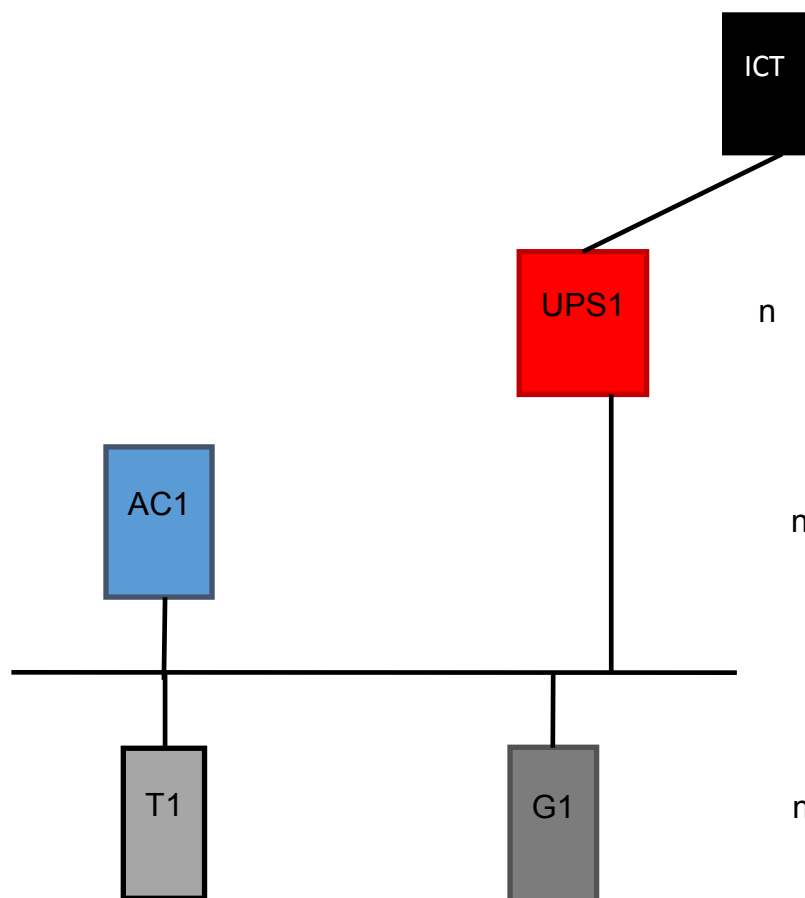
DC Tier I je náchylné na prerušenia prevádzky z dôvodov porúch alebo pri údržbe. Obsahuje len základný systém elektrického napájania a chladenia, ktorého komponenty však nie sú redundantné a počas servisu alebo poruchy je celá infraštruktúra vrátane IT mimo prevádzky. Napájacie vetvy nie sú redundantné. Kritické situácie si môžu vyžadovať viacej ukončení a opätovných spustení prevádzky. Topológia obsahuje viacero SPOF. Výpadok DC je cca 28,8 hod. ročne mimo plánovaných odstávok, čo predstavuje dostupnosť 99,67%.

Základné parametre:

- Neredundantné komponenty
- Neredundantné rozvodné trasy

Vplyv na prevádzku:

- Prevádzka je prerušená z dôvodu poruchy komponentu alebo rozvodnej trasy
- Prevádzka je prerušená z dôvodu pravidelnej údržby
- V prípade poruchy môže nastať viacero reštartov systému



Obrázok 6 Příklad zjednodušené topologie Tier I

Tier II

V topológii Tier II infraštruktúra obsahuje redundantné komponenty. Distribučné vetvy nie sú redundantné. Porucha alebo údržba na rozvodnej trase má za následok prerušenie prevádzky IT.

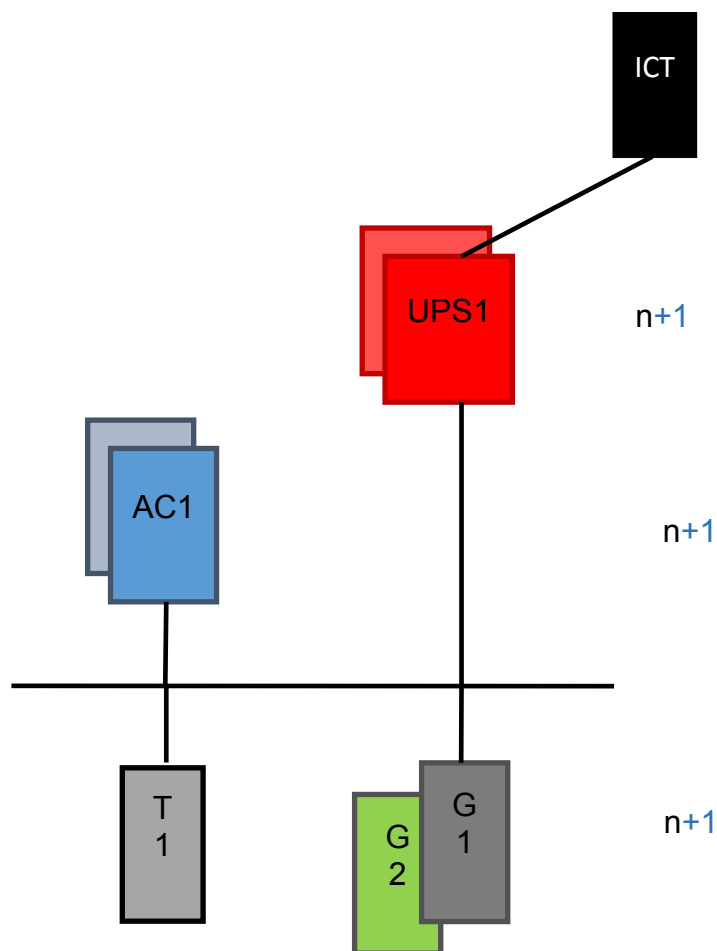
Topológia obsahuje viacero SPOF. Výpadok DC v roku je cca 22 hod. ročne mimo plánovaných odstávok, čo predstavuje dostupnosť 99,75%.

Základné parametre:

- Topológia obsahuje redundantné UPS,
- Neredundantné rozvodné trasy a motor generátor.

Vplyv na prevádzku:

- Prevádzka môže byť prerušená z dôvodu poruchy na komponente
- Prevádzka môže byť prerušená z dôvodu pravidelnej údržby na rozvodnej trase
- Prevádzka je prerušená z dôvodu poruchy na rozvodnej trase
- Prevádzka je prerušená z dôvodu pravidelnej údržby na rozvodnej trase



Obrázok 7 Príklad zjednodušenej topológie Tier II

Tier III

Topológia Tier III využíva dve napájacie vetvy aktívnu a pasívnu. Zaisťuje servisovateľnosť DC počas prevádzky. To znamená, že podporné technológie DC je možné servisovať bez nutnosti odstavenia IT prevádzky. Obsahuje redundantné komponenty a viacnásobné rozvodné trasy. V princípe je odolná proti jednej neplánovanej udalosti na infraštruktúre avšak obsahuje SPOF, ktorého porucha môže byť príčinou prerušenia prevádzky.

Základné parametre:

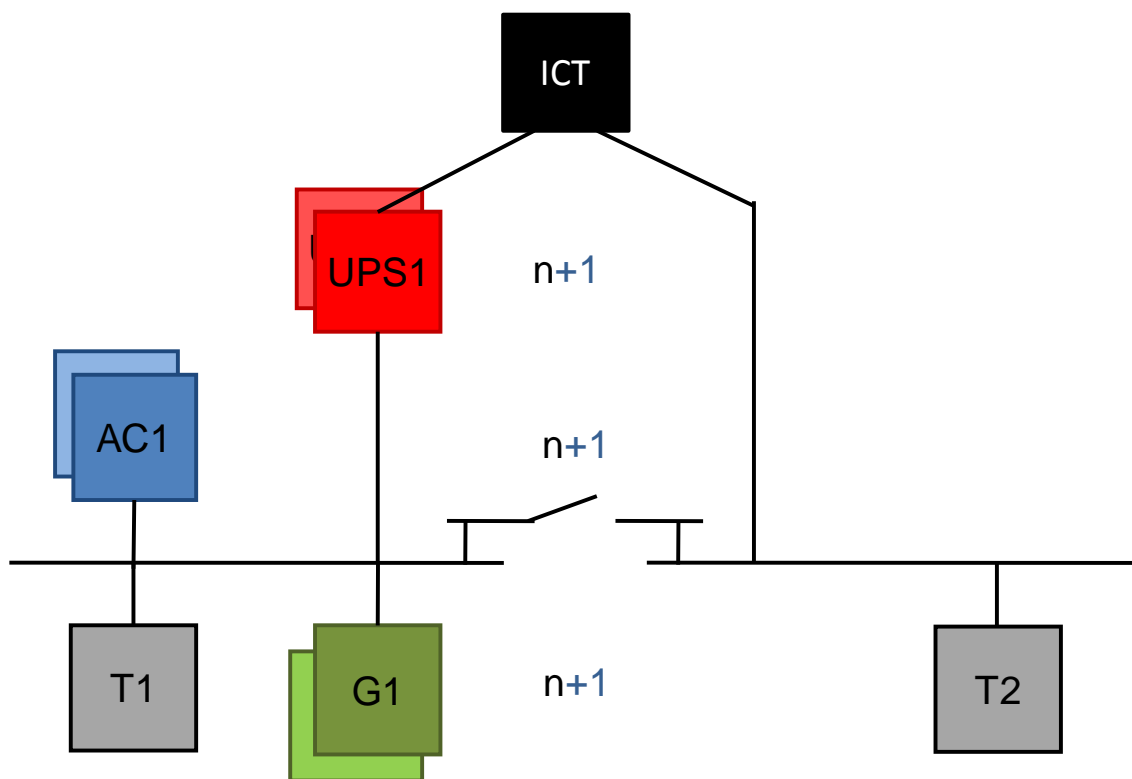
- Topológia obsahuje redundantné energetické aktívne komponenty (UPS, motor generátor, komponenty chladenia)
- Redundantné rozvodné elektrické trasy a trasy chladenia

Vplyv na prevádzku:

- Prevádzka nie je náchylná na prerušenie z dôvodu jednej neplánovanej udalosti
- Prevádzka nemusí byť prerušená z dôvodu pravidelnej údržby
- Údržba môže byť prevádzaná bez odstávky s využitím redundancie komponentov
- Prevádzka môže byť prerušená pri jednej poruche
- Prevádzka môže byť prerušená z dôvodu ľudskej chyby
- Prevádzku môže prerušiť požiarny poplach, hasenie alebo EPO

Výpadok DC v roku je cca 1,6 hod. ročne mimo plánovaných odstávok, čo predstavuje dostupnosť 99,98%.

Topológia Tier III je odporúčaná ako referenčná pre návrh riešenia so zvýšeným stupňom redundancie UPS z $n+1$ na $2(n+1)$.



Obrázok 8 Príklad zjednodušenej topológie Tier III

Tier IV

The Uptime Institute definuje požiadavky na topológiu elektrického napájania dátového centra pre kategóriu Tier IV v dvoch nezávislých aktívnych vetvách. Ostatné aktualizované požiadavky už nevyžadujú dva nezávislé VN/NN prípojky do objektu. Redundancia je posudzovaná od úrovne napájania z motor generátora. Obidve vetvy sú zálohované vlastnou skupinou UPS a motor generátorov v redundancii N alebo $N+1$ pre dosiahnutie celkovej redundancie $2S/2n$ prípadne $2(N+1)$ s primárnym cieľom zaistiť počet funkčných komponentov N pri akejkoľvek jednej chybe. Rozloženie výkonu na jednotlivé vetvy je rovnomerné, pričom každá vetva môže byť zaťažená maximálne na 50%, aby mala dostatočnú výkonovú kapacitu na prevzatie celej záťaže v prípade poruchy alebo servisu, ktorý má za následok odstavenie druhej vetvy.

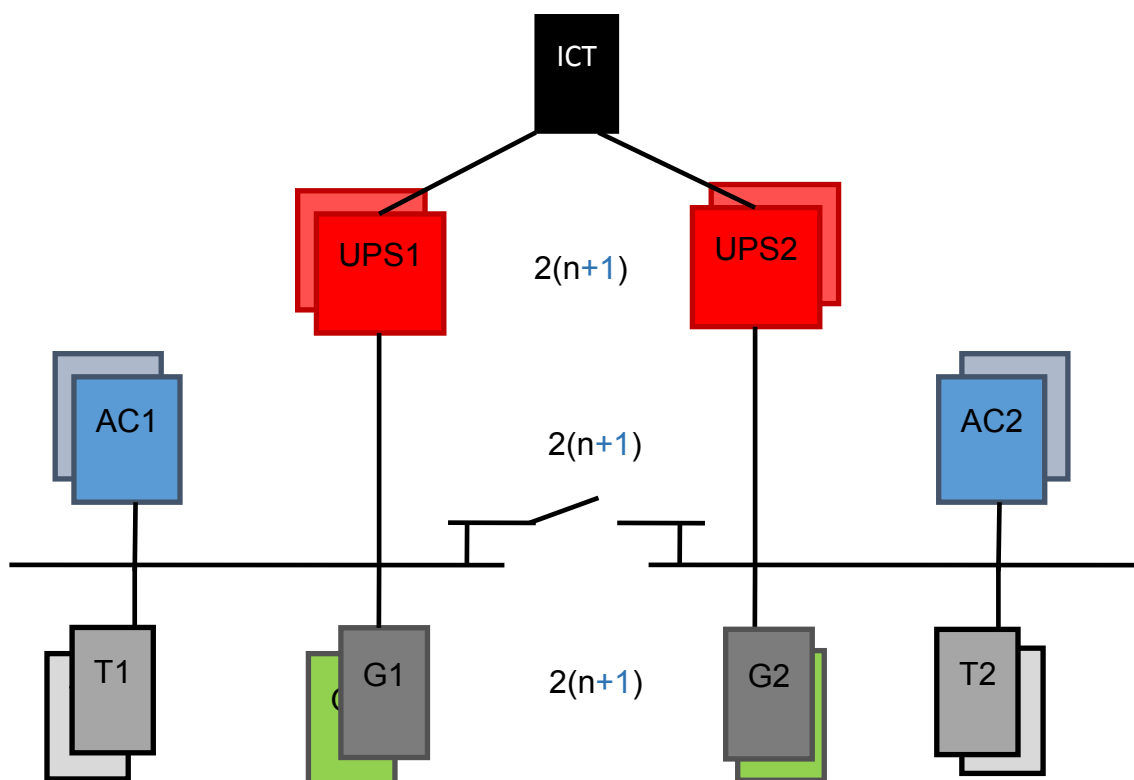
Základné parametre:

- Topológia obsahuje dve aktívne vetvy
- každá vetva má dostatočnú kapacitu na prevzatie výkonu z druhej vetvy v prípade jej poruchy alebo počas údržby
- Viacnásobné rozvodné trasy
- Zdvojené zdroje IT, každý napájaný z inej vetvy

Vplyv na prevádzku:

- Prevádzka IT nie je náchylná na prerušenie z dôvodu jednej neplánovanej udalosti
- Prevádzka nemusí byť prerušená z dôvodu pravidelnej údržby
- Údržba môže byť prevádzaná bez odstávky s využitím redundancie komponentov
- Prevádzka IT nie je prerušená pri jednej poruche
- Prevádzka môže byť prerušená z dôvodu ľudskej chyby
- Prevádzku môže prerušiť požiar, poplach, hasenie alebo EPO.

Výpadok DC v roku je cca 0,8 hod. ročne mimo plánovaných odstávok, čo predstavuje dostupnosť 99,99%.



Obrázok 9 Príklad zjednodušenej topológie Tier IV

TIA-942

Organizácia The Telecommunications Industry Association vydala dokument TIA-942 - Telecommunications Infrastructure Standards for Data Centers, kde je komplexne spracovaná problematika dátových centier. Pri kategorizácii DC vychádza z kategorizácie The Uptime Institute. Dátové centrá rozdeľuje na 4 skupiny Tier 1 – 4 podľa ich miery dostupnosti a zabezpečenia. Na rozdiel od The Uptime Institute používa arabské číslce. Pre účely definovania požiadaviek sú vybrané parametre uvedené nasledovnej tabuľke.

Tabuľka 5 Vybrané parametre podľa TIA-942

Položka	Tier 1	Tier 2	Tier 3	Tier 4	Požiadavky na DC
Požiarna odolnosť, vonkajšie steny	v zmysle lokálnej legislatívy	v zmysle lokálnej legislatívy	Min 1 hod	Min 4 hod.	min REI60 EN 1634
Požiarna odolnosť, vnútorné steny	v zmysle lokálnej legislatívy	v zmysle lokálnej legislatívy	Min 1 hod	Min 1 hod.	min REI60 EN 1634
Požiarna odolnosť, vnútorné steny IT sály	v zmysle lokálnej legislatívy	v zmysle lokálnej legislatívy	Min 1 hod	Min 2 hod.	min REI60 EN 1634
Požiarna odolnosť, dvere do IT sály	v zmysle lokálnej legislatívy	v zmysle lokálnej legislatívy	45 min	90 min	min EW60 podľa EN 1634
Rozmer dverí (š x v)	1m x 2,13m	1m x 2,13m	1m x 2,13m	1,2m x 2,13m	1,2m x 2,13m
Výška stropu	Min 2,6m	Min 2,7m	3m	3m	3m
Kapacita palivového hospodárstva	8 hod (generátor sa nepožaduje, ak UPS má údobu zálohovania viac ako 8 min)	24 hod	72 hod	96 hod	48 hod

BICSI

Organizácia BICSI publikovala dokument BICSI 002-2011, Data Center Design and Implementation. V uvedenom dokumente sú komplexne spracované princípy riešenia DC. Dátové centrá klasifikuje do kategórií Class F0 – F4. Pre definovanie požiadaviek na DC tieto neboli aplikované, nakoľko sa jedná o obdobné požiadavky ako TIA-942.

4.3.3.2 Priestorové a výkonové požiadavky

Priestorové a výkonové požiadavky na Dátové centrum sú definované za predpokladu vybudovania dvoch dátových sál s približne rovnakou IT plochou cca 400 m² pre každú sálu (viď kapitolu 4.2 Analýza požiadaviek a potrieb stakeholderov). K tomu sú predpokladané ďalšie potrebné priestory vychádzajúce z bežnej praxe.

Detailnejšie požiadavky pre jednu dátovú sálu sú uvedené v nasledovnej tabuľke (všetky hodnoty sú orientačné a založené na predpokladoch, reálne čísla v projekte môžu byť iné v rámci tolerancií do 20%, prípadne zásadne iné v prípade zmeny predpokladov, resp. vstupov):

Tabuľka 6 Základné priestorové a výkonové požiadavky

Parameter	Základná požiadavka	Poznámka
Plocha IT	400 m ²	Požadovanú základnú plochu je potrebné stanoviť pre 150 rackov s dodržaním uvedených závislostí vzájomného usporiadania zariadení vo vyhradenom priestore s príslušným servisným priestorom najmenej 1,2m pred rackom a najmenej 0,9 m za rackom a transportnou plochou umožňujúcou transport ktoréhokoľvek z uvedených rackov von a na pozíciu racku. Plocha musí umožňovať rozdelenie rackov do 8 samostatných kliebok/sekcii oddelených mrežou s kontrolovaným vstupom prostredníctvom systému kontroly vstupov (SKV).
Počet rackov	150 v 8 sekciiach/ kliebkach	Typový rozmer racku je šírka 60 cm a hĺbka 120 cm.
Výkon na plochu	1,5kW/m ²	
Výkon na rack	4kW	
Súvisiace priestory podpornej infraštruktúry	V zmysle metodológie zónovania a rozdelenia redundantných komponentov a trás do oddelených požiarnych úsekov	Preferované je umiestnenie s prístupom cez vyhradenú chodbu s kontrolovaným vstupom prostredníctvom systému kontroly vstupov (SKV)
Kancelária - vedúci pracovník	2 pracovné miesta	Preferované je umiestnenie s prístupom cez vyhradenú chodbu s kontrolovaným vstupom prostredníctvom systému kontroly vstupov (SKV)
Kancelária – pracovníci	5 pracovných miest	Preferované je umiestnenie s prístupom cez vyhradenú chodbu s kontrolovaným vstupom prostredníctvom systému kontroly vstupov (SKV)
Miestnosť operátorov	2 pracovné miesta	Preferované je umiestnenie s prístupom cez vyhradenú chodbu s kontrolovaným vstupom prostredníctvom systému kontroly vstupov (SKV)
Technologický dohľad	2 pracovné miesta	
Sklad – IT	12 m ²	Preferované je umiestnenie v blízkosti IT sály s kontrolovaným vstupom prostredníctvom systému kontroly vstupov (SKV). Požadovaná plocha môže byť aj v dvoch miestnostiach.
Sklad - podporná infraštruktúra	12 m ²	

Sklad - kancelária	10 m ²	Preferované je umiestnenie s prístupom cez vyhradenú chodbu s kontrolovaným vstupom prostredníctvom systému kontroly vstupov (SKV)
Rokovacia miestnosť	12 osôb	V základnej požiadavke môže byť v prenajatých priestoroch, preferované vlastná miestnosť. V prípade rozšírenia vlastná.
Sociálne zariadenia a kuchynka		Môžu byť v prenajatých priestoroch. Preferované vlastné.

4.3.3.3 Východiská riešenia pre Ministerstvo vnútra SR

Vzhľadom na fakt, že v Banskej Bystrici a okolí (požadovaná lokalita dátového centra) sa nenachádzajú vhodné dátové centrá, u ktorých by bolo možné uvažovať nad ich kúpou, boli pre účely analýzy možností vybudovania dátového centra MV SR vybrané viaceré jestvujúce objekty vo vlastníctve rezortu. Následnou selekciou bol zvolený trojpodlažný objekt v areáli sekcie IZS (Integrovaný záchranný systém) v katastri obce Slovenská Ľupča pozostávajúci z častí C, D, E, F. Hlavná časť objektu tvorí časť C pôdorysných rozmerov cca 67m x 15,5m. Jedná sa o trojtrakt, kde nosný systém je tvorený železobetónovým skeletom s konštrukčnými výškami 4,6m; 3,85m a 3,85m. Časti D,E,F napojené kolmo na časť C sú od nej dilatčne oddelené. Zastrešenie všetkých častí objektu je plochou strechou.

Výhody vybraného objektu sú nasledovné:

- Jestvujúca samostatne stojaca budova v chránenom areáli vo vlastníctve a správe rezortu
- Akceptovateľná vzdialenosť od ostatných dátových sál rezortu (lokalita Timrava v Banskej Bystrici a Tajov)
- Jestvujúca VN prípojka v areáli
- Jestvujúce optické pripojenie
- Dostatočná svetlá výška (390 cm) miestností na prízemí pre účely dátového centra
- Možnosť prebudovania vnútornej dispozície priestoru pre účely DC s aplikovaním princípu zónovania
- Dostatok miesta a vhodná svetlá výška konštrukčného systému pre vybudovanie IT pracovísk na 2NP a 3NP
- Prvé nadzemné podlažie (1NP) časti C, vhodné pre umiestnenie dátového centra, je jednoducho bezpečnostne a oddeliteľné od ostatných častí objektu
- Priestorové usporiadanie a osadenie objektu C je vhodné z hľadiska minimálneho ohrozenia zaplavením vzhľadom na polohu budovy
- Objekt má vhodne riešený prekrytý prejazd, umožňujúci jednoduché navážanie technologických zariadení aj počas zlých poveternostných podmienok

Pre dosiahnutie požadovaných priestorových a výkonových požiadaviek v príslušných štandardoch dátového centra je potrebné v objekte zrealizovať stavebné a technologické úpravy. Tie sú stručne popísané v nasledovných odsekoch, pričom tieto úpravy sú aj podkladom pre

plánovaný rámcový rozpočet projektu. Konkrétne hodnoty môžu byť pri prípadnom projekte upravené na základe detailného návrhu projektu stavby resp. technológie.

Stavebné úpravy

Pre adaptáciu objektu na dátové centrum je potrebné zrealizovať komplexnú stavebnú rekonštrukciu objektu. V návrhu priestorového členenia budú aplikované zásady metodológie budovania dátových centier, ako napr. systém zónovania s oddelením priestorov IKT od priestorov podpornej infraštruktúry. Redundantné komponenty podpornej infraštruktúry budú v rámci priestorových možností oddelené do samostatných požiarnych úsekov. Vstup do objektu bude osobitne riešený pre osoby a technológiu. IKT sála bude z bezpečnostných dôvodov bez okien.

Deliace konštrukcie a bezpečnostné dvere budú v súlade s požiadavkami tohto dokumentu na bezpečnostnú triedu a požiarnu odolnosť. Rozmery transportných trás budú umožňovať prepravu objemných technologických zariadení. V priestore DC bude inštalovaná zdvojená podlaha, ktorá bude slúžiť na distribúciu chladeného vzduchu v priestore IT sály a uloženie energetických rozvodov v elektrorozvodniach.

Adaptácia predpokladá aj rekonštrukciu strešného plášťa.

Horné podlažia (2NP a 3NP) budú využité pre IT prevádzku.

Elektrické napájanie

Predpokladá sa vybudovanie kompletných elektrických rozvodov od jestvujúcej VN prípojky v členení:

- 2 vetvy aktívna-aktívna napájanie IT
- 2 vetvy aktívna-pasívna napájanie chladenia
- žľabový systém pre štruktúrovanú dátovú kabeláž
- osvetlenie priestorov IKT, podporných technológií, IT pracovísk a ostatných dotknutých priestorov
- uzemnenie a bleskozvod, obnova v zmysle súčasných platných noriem
- transformátor, vyhradený len pre účely DC
- VN prípojka k novovybudovanému transformátoru
- IT pracoviská, zálohované a nezálohované napájanie z UPS

Nepretržité napájanie IT technológií bude zaistené prostredníctvom UPS:

- výkon 650 kW
- doba zálohovania 10 minút
- redundancia 2(n+1)

Rozvody budú doplnené náhradnými zdrojmi – motorgenerátormi o predpokladaných parametroch:

- 2 x 1,5 MW prime výkon
- redundancia n+1
- palivové hospodárstvo 48 hod.

Navrhovaná topológia zodpovedá štandardu Tier III pre podpornú infraštruktúru. Napájanie IT dvomi aktívnymi vetvami a redundanciou UPS zodpovedá štandardu Tier IV. Elektroinštalačné rozvody sú požadované v päťvodičovej sústave TNS s jedným bodom prepojenia medzi vodičmi PE a N.

Pokiaľ to priestorové podmienky umožnia, budú požiarne oddelené redundantné vetvy a redundantné komponenty elektrického napájania.

Chladenie

Technológia chladenia zabezpečí chladenie, zvlhčovanie a odvlhčovanie priestoru novej DC sály podľa požiadaviek na prevádzku IT technológií nasledovne:

- cirkulačné vetranie, priame chladenie a zvlhčovanie – IT sála
 - tepelná záťaž priestoru 650 kW
 - celoročná teplota v miestnosti 22 ± 2 C
 - celoročná relatívna vlhkosť v miestnosti – ϕ 40%- 60%
 - stupeň redundancie n+1
 - delenie vnútorného priestoru na tzv. teplé a studené uličky v nadväznosti na osadenie technologických zariadení
 - vnútorné stojace jednotky s presnou reguláciou teploty a vlhkosti, projektované parametre musia zaistiť prevádzku počas celého teplotného rozsahu vonkajšieho prostredia v danej lokalite
- chladenie UPS
 - tepelná záťaž priestoru cca 265 kW
 - celoročná teplota v miestnosti 22 ± 2 C
 - stupeň redundancie n+1
- IT pracoviská
 - riešenie VZT bude zaisťovať kúrenie na IT pracoviskách. Vetranie bude riešené oknami.

Vo všeobecnosti bude návrh chladenia IKT v súlade s dokumentom ASHRAE, 2011 Thermal Guidelines for Data Processing Environments - Expanded Data Center Classes and Usage Guidance)

Bezpečnostné systémy

Objekt bude vybavený bezpečnostnými systémami:

- PSN - poplachový systém narušenia
- SKV - systém kontroly vstupov
- PTV - priemyselná TV
- DZ - detekcia zatečenia

Uvedené systémy budú integrovateľné s jestvujúcimi v súčasných dátových centrách.

Požiarna ochrana

Systémy pre požiaru ochranu IT a podporných technológií

- EPS - elektronická požiaru signalizácia
- SDP - skorá detekcia požiaru, IT sály
- SHZ - stabilné hasiace zariadenie IT sály, UPS miestnosti

Systémy požiarnej ochrany budú v zmysle platnej legislatívy s možnosťou integrácie do jestvujúcich systémov v súčasných DC.

Monitoring

Všetky technologické a bezpečnostné systémy budú na nadradenej úrovni prepojené do centrálneho monitoringu, ktorý bude integrovať technologické dáta a poskytovať v reálnom čase informácie pre obsluhu na dispečerskom pracovisku. Obsluha bude mať prístup z lokálneho pracoviska v objekte, v prípade potreby aj so vzdialeného záložného pracoviska prepojeného v jednotnej sieti.

Monitoring bude pozostávať z technických prostriedkov pre prenos a vyhodnotenie zbieraných údajov z jednotlivých technológií, ich grafickú prezentáciu, logovanie, archiváciu a reporting.

4.4 Definície služieb

Vzhľadom na odlišný charakter od ostatných projektov OPIS PO1 nie je možné definovať služby spôsobom, ktorý sa využíva pre ostatné projekty. Dôvodom je orientácia projektu striktne na infraštruktúru bez implementácie informačných systémov. Táto infraštruktúra však bude nevyhnutným predpokladom na prevádzkovanie informačných systémov a teda poskytovanie ich eGov a IS služieb.

Napriek vyššie uvedenej skutočnosti výsledkom projektu bude poskytovanie služieb, len ich charakter nie je možné presne zachytiť formou eGov a IS služieb a tieto služby nebudú poskytované verejnosti (občanom ani podnikateľom) ale pôjde o technologické služby zabezpečenia a poskytovania infraštruktúry iným subjektom verejnej správy. Tieto služby sú

popísané v kapitole [Služby dátového centra](#). Popísané služby však nebudú predmetom výzvy ako povinné služby implementované v projekte a nebudú pokladom na CBA analýzu, keďže nejde o služby doteraz poskytované iným spôsobom a týmto projektom elektronizované.

4.5 Uskutočniteľnosť a náklady

4.5.1 Dopady na technické a softwarové vybavenie

Dopady zavedenia nového dátového centra do prostredia systémov verejnej správy sú zásadné a vyžadujú dôkladné plánovanie a vykonanie všetkých potrebných krokov. Okrem aspektov analyzovaných v samostatných ďalších kapitolách ide z technického pohľadu o pokrytie minimálne nasledovných oblastí:

- Zaintegrovanie DC na úrovni základnej infraštruktúry – najmä siet'ovej
- Rozvrhnutie a príprava dátového centra podľa potrieb budúcich používateľov najmä z pohľadu kapacitných a bezpečnostných požiadaviek – dopad na rozdelenie plochy dátového centra na fyzicky oddelené oblasti („klietky“) tam, kde je to nevyhnutné
- Návrh cieľovej architektúry informačných systémov ktoré budú v cieľovom DC prevádzkované vzhľadom na nový prvok v infraštruktúre – najmä z pohľadu topológie nasadenia informačných systémov. Primárne predpokladáme:
 - Pre nové informačné systémy – umiestnenie jedného z uzlov nasadenia (či už primárneho alebo sekundárneho) do predmetného DC
 - Pre existujúce informačné systémy – migráciu do predmetného DC, resp. migráciu jedného z uzlov nasadenia pre dosiahnutie vyššej dostupnosti, bezpečnosti resp. výkonu.
- Detailný návrh IKT – HW a SW prevádzkovaného v DC. Tu môže ísť o kombináciu existujúcich IKT, ktoré budú sťahované do nového DC a nových IKT, ktoré budú zabezpečovať budúcu prevádzku
- Samotná migrácia resp. nasadenie informačných systémov – po dôslednom naplánovaní všetkých krokov a ich adekvátnom overení skúškami a testovaním bude potrebné zrealizovať samotnú migráciu a nasadenie tak, aby sa zabezpečil minimálny dopad na prevádzku existujúcich systémov a prípadný dopad bol vopred odsúhlasený s príslušnými zainteresovanými stranami

4.5.2 Organizačné dopady

4.5.2.1 Interná organizácia

Zabezpečenie poskytovania služieb Dátového centra bude vyžadovať internú organizáciu, ktorá musí adresovať oblasti:

- riadenia
- podpory (obsluhy)

- architektúry

Požiadavky na ľudské zdroje sú rozdelené na bežnú prevádzku a pohotovosť. Bežná prevádzka je definovaná v rámci pracovných dní počas jednej 8 hodinovej zmeny v mieste dátových centier alebo na to určených administratívnych priestorov. Výnimkou je dohľad (prvá úroveň obsluhy), pre ktorú je definovaná nonstop prevádzka. Pohotovosť nemá obmedzenie v čase a je poskytovaná telefonicky mimo pracovnú zmenu. Ľudské zdroje počas pohotovosti spravidla nie sú prítomné v dátovom centre a neplnia žiadne rutinné úlohy. V prípade požiadavky na odstránenie poruchy musia zasiahnuť podľa vopred definovaných procedúr a v definovanom čase.

Obsluha prvej úrovne je zdieľaná pre všetky špecializácie a je poskytovaná operátormi dohľadového centra bez špecifických požiadaviek na ich spôsobilosti (LAN/WAN/SAN/dátové úložiská, siete a podobne). Je zodpovedná za dohľad, rutinnú prevádzku, riadenie a eskaláciu vzniknutých problémov na obsluhu druhej úrovne.

Obsluha druhej úrovne predstavuje špecialistov, ktorí sú v rámci svojej špecializácie zodpovední za návrh, plánovanie, technickú podporu, nasadenie a prevádzku komponentov IKT.

Obsluha tretej úrovne bude zabezpečovaná dodávateľsky prostredníctvom servisného kontraktu s definovanými SLA. Obsluha tretej úrovne je zodpovedná za servisnú údržbu, odstraňovanie chýb eskalovaných podporou druhej úrovne a prípadnú iniciálnu konfiguráciu IKT komponentov.

Riadenie a architektúru dátových centier bude potrebné zabezpečiť v rámci pracovných dní počas jednej 8 hodinovej zmeny v mieste dátových centier alebo na to určených administratívnych priestorov.

4.5.2.2 Externé vzťahy

Väzby Dátového centra s externými organizáciami je možné rozdeliť na vzťahy s:

- poskytovateľmi služieb
- odberateľmi služieb

Pod poskytovateľmi služieb sa primárne rozumejú externé subjekty, ktoré budú pre Dátové centrum zabezpečovať podporu a údržbu IKT infraštruktúry a informačných systémov. Vzájomné vzťahy budú formálne riadené zmluvami o poskytovaní služieb. Kvalita odoberaných služieb bude priebežne monitorovaná a vyhodnocovaná voči zmluvne definovaným podmienkam. Za aktuálnosť a finančnú efektívnosť týchto zmlúv bude zodpovedný manažér prevádzky Dátového centra.

Odberateľmi služieb Dátového centra budú v zmysle cieľov tejto štúdie organizácie verejnej správy, ktoré spravujú svoje ISVS. Vzhľadom na celkovú komplexnosť prostredia verejnej správy bude nasadenie služieb Dátového centra vyžadovať dôslednú koordináciu a riadenie minimálne na úrovni:

- strategické plánovanie - definuje záväzný plán pre zabezpečenie konzistencie medzi jednotlivými projektmi a inými aktivitami správcov ISVS a prevádzkovateľom Dátového

centra ako nadrezortným poskytovateľom centrálnych služieb dátového centra pre elektronizáciu verejnej správy. Plánovanie a koordinácia zohľadňuje okrem iného aj to, že IKT infraštruktúra dodávaná v rámci jednotlivých projektov môže byť súčasťou celkovej zdieľanej infraštruktúry Dátového centra.

- presadenie a výkon stratégie – riadi výkon stratégie voči jednotlivým správcom ISVS (monitoruje projekty, vyhodnocuje súlad so stanovenou stratégiou, poskytuje súčinnosť, ...). Definuje štandardy pre IKT infraštruktúru, rieši konflikty a prípadné prekryvy medzi projektmi.
- pripojenie žiadateľa – riadi pripájanie žiadateľa k odberu služieb. Súčasťou je detailná analýza požiadaviek, špecifikácia požadovanej úrovne služieb, nasadenie služieb, overenie pripravenosti na strane odberateľa, testovanie a bezpečnostný/výkonnostný audit.

Kompetenciu na realizáciu hore uvedených aktivít predpokladáme na strane DataCentra, na ktoré ju deleguje MF SR ako ústredný orgán štátnej správy pre oblasť informatizácie spoločnosti, bližšie viď „Štúdia uskutočniteľnosti projektov prioritnej osi č. 1 Elektronizácia verejnej správy a rozvoj elektronických služieb Operačného programu Informatizácia spoločnosti zameranej na rozvoj komunikačno-technologickej infraštruktúry informačných systémov verejnej správy na centrálnej úrovni“ vypracovaná spoločnosťou Logica.

Pri rešpektovaní podmienok kladených na infraštruktúru môže ktorákoľvek zúčastnená strana navrhnúť a presadiť riešenie voči druhej strane. V prípade ak nevznikne dohoda je právo a povinnosť zvoliť riešenie na strane arbitra, ktorým bude na základe svojej riadiacej kompetencie MF SR.

Celková koordinačná, riadiaca a kontrolná kompetencia nad Dátovým centrom bude realizovaná MF SR, ktoré bude v jej intenciách:

- definovať minimálny rozsah štandardných služieb, ktoré bude Dátové centrum poskytovať
- definovať parametre a cenové hranice jednotlivých štandardných služieb
- definovať kvalitatívne parametre, ktoré budú musieť Dátové centrum splniť v stanovenej lehote
- rozhodovať o umiestnení aplikácií v Dátovom centre
- kontrolovať kvalitu Dátového centra
- kontrolovať rozsah a kvalitu poskytovaných služieb

4.5.3 Legislatívne dopady

Realizácia projektu nemá priame dopady na legislatívu, bližšie viď kapitolu 4.1 Legislatívna analýza.

Z pohľadu špecifik projektu, ktorým je vybudovanie Dátového centra, je nevyhnutné riešiť právne otázky spojené s vlastníctvom nehnuteľnosti. Vzhľadom na fakt, že plné vybudovanie samostatného dátového centra ako celej budovy je zložitý variant, predpokladáme v tejto analýze právnych aspektov kúpu dátového centra s požadovanými parametrami a v predpokladaných lokalitách. Z aktuálnej analýzy dátových centier v Bratislave a okolí vyplýva,

že je potrebné predpokladať aj kúpu časti nehnuteľnosti, nielen celého dátového centra (viď analýzu v kapitole 4.6.3), čo prináša isté dodatočné potreby zmluvného ošetrovania.

Pri kúpe časti dátového centra je nevyhnutné dôkladne právne ošetriť využitie zdieľaných priestorov a služieb a možnosti nakladania a úprav so samotnou kupovanou časťou.

Pod využívaním zdieľaných priestorov sa primárne rozumejú prístupové a iné komunikácie, parkoviská, spoločné priestory ako recepcia a podobne, v prípade poschodových budov výťahy.

Zdieľanými službami sú napr. stráženie a fyzické monitorovacie systémy, ale najmä v prípade, že nie sú priamou súčasťou kupovanej časti nehnuteľnosti aj technológie súvisiace s napájaním a jeho zálohovaním, chladiace technológie.

Nevyhnutnosťou je potreba definovania spôsobu merania spotreby a podieľania sa na spoločnej spotrebe médií ako elektrická energia, voda, plyn.

Pre variant adaptácie existujúcich priestorov vo vlastníctve budúceho realizátora Dátového centra (predpokladaný scenár pre MV SR) je situácia z toho pohľadu jednoduchšia a je potrebné riešiť len úkony typické pre stavebné konanie.

4.5.4 Prevádzkové a bezpečnostné dopady

Vzhľadom na fakt, že DataCentrum aj MV SR už v súčasnosti prevádzkujú dátové centrá s porovnateľnými parametrami ako je predpokladané cieľové dátové centrum, nie sú predpokladané zásadné dopady na prevádzku a bezpečnosť.

Znásobenie Datacentrom prevádzkovanej infraštruktúry na takmer 3-násobok a prípadná inštalácia kritických systémov vyžadujúcich nepretržitú podporu ako eHealth ako aj významný rast prevádzkovanej infraštruktúry na MV SR však prinesie so sebou nároky na zvýšenie počtu zamestnancov, ktorí budú túto infraštruktúru prevádzkovať, čo môže mať za následok aj proporčné navýšenie ostatného personálu. Zvýšenie počtu zamestnancov bude takisto čiastočne spôsobené aj zavedením ďalšej fyzickej lokality do architektúry.

Zásadnejšie zmeny v modeloch prevádzky aj bezpečnosti je možné očakávať pri zavádzaní cloud platformy.

4.5.4.1 Vzťah medzi Tier a prevádzkovou údržbou v zmysle The Uptime Institute

Inštalovaná podporná technológia v definovanej Tier kategórii určuje vplyv na prevádzku IT počas servisu jednotlivých komponentov alebo trás.

V prípade Tier I servis na trase alebo komponente môže spôsobiť prerušenie prevádzky IT.

Tier II umožňuje servis redundantných zariadení bez prerušenia prevádzky IT. Servis komponentov distribučných trás môže mať za následok nutnosť prerušenia IT prevádzky.

Iba podporná technológia na úrovni Tier III a IV umožňuje priebežnú servisovateľnosť každého zariadenia a komponentu distribučných trás bez nutnosti odstávky IT.

Vzhľadom na uvedené skutočnosti je pre zaistenie spojitosti obchodných činností odporúčané DC v kategórii najmenej na úrovni Tier III.

Vybrané parametre prevádzkovej údržby v zmysle The Uptime Institute

Položka	Tier I	Tier II	Tier III	Tier IV	Požadované DC
Prítomnosť personálu	Personál alebo externý poskytovateľ počas pracovného času na dohľad kritických prevádzkových úkonov	Jedna zmena počas pracovných dní, definované eskalačné procedúry	Definované eskalačné procedúry, 1 pracovník počas 7x24 hod	Definované eskalačné procedúry, 2 pracovníci počas 7x24 hod	Definované eskalačné procedúry, 1 pracovník počas 7x24 hod.
Preventívna údržba	Definovaný plán s uvedenými úkonmi a záznamom výkonov	Tier I Výkonávaná autorizovaným poskytovateľom podľa odporúčaní výrobcu	Tier II Definované postupy prepínania medzi redundantnými komponentmi Aplikovaný proces riadenia kvality	Tier II Definované postupy prepínania medzi redundantnými komponentmi Aplikovaný proces riadenia kvality	Definovaný plán s uvedenými úkonmi a záznamom výkonov Výkonávaná autorizovaným poskytovateľom podľa odporúčaní výrobcu Definované postupy prepínania medzi redundantnými komponentmi Aplikovaný proces riadenia kvality
Podpora kvalifikovaných servisných organizácií	Zoznam organizácií dostupných pre výkon servisu	Tier I Definovaná úroveň služby (SLA), harmonogram preventívnej údržby, definované doby odozvy pre kritické systémy	Tier II Poskytovanie zásahu „na zavolanie“, definovanie kontaktných miest na poskytovateľov	Tier II Poskytovanie zásahu „na zavolanie“, definovanie kontaktných miest na poskytovateľov	Zoznam organizácií dostupných pre výkon servisu Definovaná úroveň služby (SLA), harmonogram preventívnej údržby, definované doby odozvy pre kritické systémy Poskytovanie zásahu „na zavolanie“, definovanie kontaktných miest na poskytovateľov
Analýza porúch		Zoznam všetkých porúch spôsobujúcich prerušenie prevádzky IT a ponaučenia	Tier II Definovaný proces na zisťovanie príčin porúch, definovanie ponaučení a implementáci a opravných opatrení	Tier III Aplikovaný „Trend analysis“ proces	Zoznam všetkých porúch spôsobujúcich prerušenie prevádzky IT a ponaučenia Definovaný proces na zisťovanie príčin porúch, definovanie ponaučení a implementácia opravných opatrení

4.5.4.2 Riadenie informačnej bezpečnosti

Zavedenie SMIB by malo byť realizované v týchto etapách:

- vypracovanie bezpečnostného projektu
- zavedenie bezpečnostných procesov a implementácia bezpečnostných opatrení

- príprava na predcertifikačný audit
- certifikačný audit

Vypracovanie bezpečnostného projektu sa zaoberá identifikáciou a ohodnotením bezpečnostných rizík a spracovaním vrcholovej bezpečnostnej politiky, ktorá popíše organizáciu bezpečnosti a základné princípy riadenia informačnej bezpečnosti dátového centra. Realizácia bude rozdelená do nasledujúcich čiastkových úloh:

- vypracovanie bezpečnostnej politiky, stanovenie organizácie riadenia informačnej bezpečnosti, stanovenie spôsobu analýzy rizík,
- analýza rizík
 - zber vstupných podkladov,
 - realizácia analýzy rizík,
 - ohodnotenie rizík a návrh správy rizika,
 - vypracovanie GAP analýzy voči ISO 27001,
 - návrh odporúčaní,
- výber cieľov riadenia a návrh bezpečnostných opatrení nariadenie rizík,
- vypracovanie vyhlásenia o aplikovateľnosti.

Zavedenie bezpečnostných procesov a implementácia bezpečnostných opatrení zabezpečí implementáciu návrhov vyplývajúcich z bezpečnostného projektu a z analýzy rizík. Opäť bude realizácia rozdelená do čiastkových úloh a to takto:

- spracovanie plánu zvládnutia rizík,
- zavedenie a implementácia bezpečnostných opatrení v týchto oblastiach
 - organizácia bezpečnosti
 - klasifikácia a kontrola aktív
 - personálna bezpečnosť
 - manažment bezpečnostných incidentov
 - fyzická bezpečnosť a bezpečnosť prostredia
 - správa a prevádzka systémov
 - riadenie prístupu a pravidlá pre používanie IS
 - vývoj a údržba systémov
 - plánovanie kontinuity činností
 - súlad s legislatívou, štandardami a normami
- školenie zamestnancov.

4.5.5 Nasadenie riešenia a marketingové požiadavky

Nakoľko predmetný projekt nie je priamo cielený na široké skupiny používateľov – občanov a podnikateľov - nie sú typické marketingové nástroje pre nasadenie projektu kritické. Komunikáciu pre širokú verejnosť je možné realizovať koordinovane s povinnými osobami zodpovednými za správu jednotlivých informačných systémov, na ktoré ich prevádzka v budúcom dátovom centre má pozitívny dopad.

Kľúčovou však bude komunikácia a marketing v rámci verejnej správy a organizácií, ktoré sú potenciálnymi používateľmi služieb nového dátového centra. Tu je potrebné zabezpečiť, aby každý potenciálny používateľ bol informovaný o existencii nového dátového centra a najmä o výhodách využívania jeho služieb zo všetkých pohľadov vrátane cenovej efektivity takéhoto riešenia.

Komunikácia by mala byť obojsmerná a prevádzkovateľ riešenia by mal aktívne využívať aj nástroje spätnej väzby a zberu dodatočných požiadaviek tak, aby bolo riešenie dostatočne flexibilné aj pre prístupenie ďalších organizácií verejnej správy k využívaniu jeho služieb.

Hlavnými nástrojmi komunikácie by teda mali byť:

- Aktívna účasť zástupcov DataCentra, resp. MV SR na odborných podujatiach s cieľom propagácie projektového zámeru
- Priama komunikácia s organizáciami verejnej správy
- Pravidelné informovanie o dianí – brífingy a newsletter.

Dostatočné využívanie dátového centra je možné a potrebné zabezpečiť aj v rámci adekvátnej kontroly verejných výdavkov smerujúcich k budovaniu podobnej infraštruktúry a tam, kde by sa prípadná podobná plánovaná investícia neukazovala ako efektívna a potrebná, zabezpečiť najefektívnejšie riešenie.

4.5.6 Cena riešenia

Realizácia Dátového centra je možná tromi spôsobmi: adaptáciou existujúcich priestorov, výstavbou nového objektu alebo kúpou existujúceho dátového centra (resp. jeho časti), ktoré vyhovuje stanoveným požiadavkám.

Všetky tri prístupy majú svoje výhody a nevýhody, z ktorých hlavné sú:

Variant A: Adaptácia priestorov v existujúcich objektoch

Výhody:

- nižšia cena stavebných prác
- jednoduchšia legislatíva a inžinierska činnosť
- možná kratšia doba realizácie v prípade vyhovujúceho objektu

Nevýhody:

- riešenie sa musí prispôbiť existujúcim priestorom

- problém s optimálnym využitím inštalovanej infraštruktúry
- negatívny vplyv stavebných prác na prevádzku, najmä v prípade ak sa jedná o využívané priestory

Variant B: Výstavba nového objektu

Výhody

- optimálny návrh objektu bez obmedzení v zmysle požiadaviek na budovanie dátových centier
- minimálny, resp. žiadny vplyv na prevádzku

Nevýhody:

- vyššia cena stavebných prác
- dlhší čas realizácie
- náročnejšia inžinierska činnosť

Variant C: Kúpa existujúceho dátového centra (resp. jeho časti)

Výhody

- minimálny čas realizácie
- zohľadnenie požiadaviek kladených na budovanie dátových centier,
- minimálny, resp. žiadny vplyv na prevádzku existujúcej IKT
- žiadna, resp. minimálna inžinierska činnosť

Nevýhody:

- pravdepodobnosť menšieho prispôsobenia špecifickým požiadavkám
- možná zastaranosť inštalovanej infraštruktúry

Pri variante C je potrebné reálne počítať aj s kúpou časti dátového centra (teda nie celého) z nasledovných dôvodov:

- Dátové centrá spĺňajúce požiadavky sú spravidla väčšie ako identifikované potreby verejnej správy
- Vlastníci/prevádzkovatelia týchto dátových centier využívajú jeho kapacitu na prevádzku svojich systémov, resp. IKT ich zákazníkov
- Cena celého dátového centra by bola oveľa vyššia

Pre vyhodnotenie alternatív boli navrhnuté a ováňované kritériá a tie následne vyhodnotené:

- finančná nákladnosť – váha 50%

- jednoznačne najdôležitejšie kritérium pre dosiahnutie efektívneho nakladania s verejnými zdrojmi
- čas implementácie – váha 30%
 - vzhľadom na aktuálne identifikované a popísané potreby vyplývajúce z aktuálneho stavu projektov OPIS ide o dôležité kritérium pre výber správnej varianty
- komplexnosť/rizikovosť riešenia – váha 15%
 - nakoľko problémy a zmaterializované riziká pri komplexnom projekte budú viesť k dodatočným nákladom napr. na prenájom alternatívnych kapacít, dodatočné migračné aktivity pre dočasné riešenie a následný prechod na trvalé riešenie, je potrebné rizikovosť zohľadniť
- organizačná náročnosť implementácie – váha 5%
 - ponúkané riešenia vyžadujú odlišný stupeň a čas zapojenia zamestnancov DataCentra do projektových aktivít a majú vplyv na jeho schopnosť pokrývať ostatné aktivity, resp. dopad do potrebného počtu zamestnancov potrebných na vykonávanie všetkých agend

Alternatívy riešenia boli na vysokej úrovni posúdené podľa definovaných kritérií a obodované bodmi od 1 do 5 pričom 1 bod znamená, že riešenie najmenej vyhovuje definovanej požiadavke a 5 bodov znamená najlepšie splnenie požiadavky.

4.5.6.1 Varianty riešenia pre DataCentrum

Pri adaptácii existujúcich priestorov je samozrejme možná veľká variabilita stavu existujúcich priestorov. Vzhľadom na analýzu priestorov, ktoré sú k dispozícii DataCentru, resp. Ministerstvu financií SR či verejnej správe v blízkosti požadovanej lokality vo všeobecnosti, neboli identifikované žiadne vhodné priestory. Preto adaptácia v tomto prípade znamená kúpu priestorov a následnú úpravu. To z tejto varianty robí najkomplikovanejšiu variantu, pretože je potrebné počítať s veľkým úsilím na uspôsobenie. Pre prípad malého uspôsobenia by už riešenie zodpovedalo variantu kúpy, keďže malé zmeny je schopný vykonať vlastník vo svojej réžii v krátkom čase a splniť tak náležitosti budúceho prípadného obstarávania.

	Adaptácia	Výstavba	Kúpa
Financie	1	5	4
Čas	1	2	5
Komplexnosť	1	3	5
Organizačná náročnosť	1	3	5
Celkové zhodnotenie	1	3,7	4,5

Z celkového vyhodnotenia vyplýva, že vzhľadom na definované kritériá a ich váhy je najvhodnejším variantom pre Datacentrum je kúpa existujúcich vyhovujúcich priestorov.

Variant výstavby vlastných priestorov by bola vhodnejšia iba ak by jediným kritériom bola finančná nákladnosť samotnej implementácie, pri pripočítaní dodatočných nákladov súvisiacich s potrebou pokryť dočasné riešenia a následnú migráciu do cieľového dátového centra na približne 3 roky (odhadovaný rozdiel v trvaní týchto dvoch možností) by ani celkový finančný náklad nebol nižší.

4.5.6.2 Varianty riešenia pre MV SR

Napriek tomu, že požiadavky pre dátové centrá pre obe organizácie sú v princípe identické, východiská sa v niektorých oblastiach zásadne odlišujú:

- V okolí Banskej Bystrice, kde sa vzhľadom na uvedené technické požiadavky predpokladá vybudovanie dátovej sály nefunguje trhové prostredie v oblasti komerčných dátových centier zodpovedajúcim požiadavkám a teda nie je možné uvažovať kúpu existujúcich priestorov.
- Časový faktor nezohráva tak významnú úlohu vzhľadom na fakt, že akútne potreby najmä prebiehajúcich projektov už môžu byť pokryté dátovou sálou Datacentra.
- MV SR disponuje nehnuteľnosťou, ktorá svojou lokalitou, stavebnou konštrukciou a základnou infraštruktúrou (dostatočný prívod elektrickej energie, optické pripojenie) umožňuje adaptáciu na dátové centrum bez významnejších obmedzení a teda významne znižuje komplexnosť aj finančnú a časovú náročnosť tohto variantu

Na základe týchto východísk po vylúčení scenára kúpy existujúceho dátového centra a významného zníženia nákladov aj času využitím vhodnej budovy vo vlastníctve MV SR je pre MV SR najvhodnejší práve variant adaptácie tejto budovy.

4.5.6.3 Odhad ceny na základe benchmarkov

Pri odhade samotnej ceny riešenia je možné vychádzať z benchmarkov The Uptime Institute, ktoré uvádzajú:

Tabuľka 7 Referenčné ceny dátových sál podľa The Uptime Institute z presnosťou 30%.

Položka	Cena bez DPH	Prepočet na EUR bez DPH ¹
Jednotková cena podpornej infraštruktúry - Tier III [cena/kW]	25,000 USD	18,776 EUR
Jednotková cena podpornej infraštruktúry - Tier IV [cena/kW]	28,000 USD	21,029 EUR
Jednotková cena plochy IT sály [cena/m ²]	2,880 USD	2,163 EUR

DataCentrum

Pri odhadovanom počte cca 150 rackov (viď 4.2 Analýza požiadaviek a potrieb stakeholderov), priemernom príkone 4 kW na rack a odhadnutej plochy dodatočných odhadovaných netechnologických priestorov je rámcový rozpočet nasledovný:

¹ Na prepočet bol použitý kurz USD k 13.6.2013 zo stránky www.nbs.sk – 1,3315

Tabuľka 8 Orientačný rozpočet projektu pre DataCentrum na základe benchmarkov

Parameter	Položka	Hodnota	The Uptime - Tier III			Poznámky
			jednotková cena bez DPH	Spolu bez DPH	Spolu s DPH	
Plocha	IT [m2]	400.00	2,163 EUR	865,200 EUR	1,038,240 EUR	
	Počet rackov [ks]	150.00			0 EUR	pri zohľadnení členenia priestoru do 8 sekcií oddelených mrežou
Výkon [kW]	IT	640.00	18,776 EUR	12,016,640 EUR	14,419,968 EUR	
	na m2	1.60			0 EUR	
Plocha - ostatné [m2]	Podporné technológie	400.00			0 EUR	obsiahnuté v cene IT plochy
	Kancelárie	70.00	1,370 EUR	95,900 EUR	115,080 EUR	
	SBS	14.00	1,370 EUR	19,180 EUR	23,016 EUR	
	Skladovacie priestory	20.00	1,370 EUR	27,400 EUR	32,880 EUR	
	Vybavenie HW	10.00	1,370 EUR	13,700 EUR	16,440 EUR	
	Nakladacia rampa	6.00	1,370 EUR	8,220 EUR	9,864 EUR	
	Ostatné (chodby, atď.)	30.00	1,370 EUR	41,100 EUR	49,320 EUR	
	Podporné aktivity			120,000 EUR	144,000 EUR	
	Publicita a informovanie			40,000 EUR	48,000 EUR	
Spolu				13,087,340 EUR	15,896,808 EUR	

V tabuľke sú zahrnuté aj odhadované náklady na podporné aktivity projektu, teda projektové riadenie a aktivity publicity a informovania o projekte. Tieto aktivity sú predpokladané v pomere k celkovému rozpočtu v menšom rozsahu ako je typické pre ostatné projekty OPIS PO1 najmä vzhľadom na predpokladané kratšie trvanie projektu.

Na základe tohto výpočtu štúdia predpokladá cena projektu na úrovni 15 miliónov EUR s DPH (presný výpočet podľa benchmarku je 15 896 808 EUR, je však možné predpokladať skôr nižšiu cenu ako určuje benchmark).

Ministerstvo vnútra SR

Vzhľadom na špecifikum projektu MV SR, teda adaptáciu existujúcej budovy na dátové centrum, bolo potrebné niektoré parametre mierne upraviť v rámci tolerancií vzhľadom na konkrétne dispozície budovy. Predpokladá sa plocha IT sály 450 m² rozdelených do 6 sekcií s možnosťou osadenia 160 rackov. Ďalšie dve nadzemné podlažia umožňujú zriadenie až 2000 m² kancelárskych priestorov, ktoré je možné využiť pre zamestnancov IT oddelení rezortu. Na tejto ploche je pri priemernej kancelárskej ploche 10m² na zamestnanca možné pripraviť priestor pre prácu približne 200 zamestnancom, čo zodpovedá výhľadovým potrebám IT zložiek rezortu. Tabuľka podobne ako pre DataCentrum obsahuje aj podporné aktivity projektu, opätovne v relatívne nižšej miere ako je typické pre ostatné OPIS projekty, avšak vyššej ako pre DataCentrum, nakoľko predpokladané trvanie projektu je dlhšie a projekt si teda vyžaduje viac úsilia na riadenie, administratívu a súvisiacu podporu.

Tabuľka 9 Orientačný rozpočet projektu MV SR na základe benchmarkov.

Parameter	Položka	Hodnota	The Uptime - Tier III			Poznámky
			jednotková cena bez DPH	Spolu bez DPH	Spolu s DPH	
Plocha	IT [m2]	450.00	2,163 EUR	973,350 EUR	1,168,020 EUR	
	Počet rackov [ks]	160.00			0 EUR	pri zohľadnení členenia priestoru do 6 sekcií oddelených mrežou
	IT rozvoj [m2]	0.00	1,370 EUR	0 EUR	0 EUR	
Výkon [kW]	IT	675.00	18,776 EUR	12,673,800 EUR	15,208,560 EUR	
	na m2	1.50			0 EUR	
Plocha - ostatné [m2]	Podporné technológie	410.00			0 EUR	obsiahnuté v cene IT plochy
	Podporné technológie - rozvoj	0.00	1,370 EUR	0 EUR	0 EUR	
	IT pracoviská	2,000.00	1,000 EUR	2,000,000 EUR	2,400,000 EUR	Obvyklá rozpočtová cena
	SBS	20.00	1,370 EUR	27,400 EUR	32,880 EUR	
	Skladovacie priestory	30.00	1,370 EUR	41,100 EUR	49,320 EUR	
	Vybalenie HW	0.00	1,370 EUR	0 EUR	0 EUR	
	Nakladacia rampa	0.00	1,370 EUR	0 EUR	0 EUR	
	Ostatné (chodby, atď.)	90.00	1,370 EUR	123,300 EUR	147,960 EUR	
Podporné aktivity	Projektové riadenie			220,000 EUR	264,000 EUR	
	Publicita a informovanie			80,000 EUR	96,000 EUR	
Spolu	Plocha [m2]	3,000.00		16,138,950 EUR	19,366,740 EUR	

Výsledná cena v tabuľke by znamenala cenu v prípade budovania dátového centra „na zelenej lúke“, čo nie je prípad projektu MV SR. Ministerstvo vnútra SR disponuje vhodnou budovou, ktorá je vybavená navyše napr. prípojkou vysokého napätia v areáli a optickým pripojením, takže cena projektu môže byť významne nižšia.

Skutočný potrebný rozpočet potrebný na realizáciu projektu bol teda vyčíslený aj ako odhad na základe odhadovaných cien jednotlivých potrebných prác potrebných na adaptáciu budovy a areálu, ktorý je presnejší a zodpovedá aktuálnej situácii projektu a budovy, ktorá bude prebudovaná:

Tabuľka 10 Odhad nákladov projektu pre MV SR

Položka	Popis	Cena bez DPH	Cena s DPH
Stavebná časť	stavebné úpravy dotknutých priestorov bezpečnostné a požiarne dvere vybudovanie bezpečnostných a požiarnych deliacich konštrukcií zdvojená podlaha, trieda 5, bodové zaťaženie 5kN výmena jestvujúcich okien úprava fasády oprava strešného plášťa stavebné úpravy presunutých pracovísk	5,770,000 EUR	6,924,000 EUR
Úpravy okolia	oplotenie, brána spevnené plochy	259,000 EUR	310,800 EUR
UPS	záložné zdroje nepretržitého napájania výkon 650 kW doba zálohovania 10 minút redundancia 2(n+1)	600,000 EUR	720,000 EUR
Elektro	2 vetvy aktívna-aktívna napájanie IT 2 vetvy aktívna-pasívna napájanie chladenia žľabový systém pre štruktúrovanú dátovú kabeláž osvetlenie bleskozvod transformátor VN IT pracoviská	1,400,000 EUR	1,680,000 EUR
MG	náhradné zdroje elektrického napájania, motor generátor, 2 x 1,5 MW prime, redundancia n+1, palivové hospodárstvo 48 hod	700,000 EUR	840,000 EUR
Chladenie, VZT	stojace chladiace jednotky s presnou reguláciou teploty a vlhkosti pre IT sálu, freecooling, redundancia n+1 stojace chladiace jednotky s presnou reguláciou teploty pre UPS a elektro rozvodne, redundancia n+1 VZT vykurovanie	1,200,000 EUR	1,440,000 EUR
Bezpečnostné systémy	PSN - poplachový systém narušenia SKV - systém kontroly vstupov PTV - priemyselná TV DZ - detekcia zatečenia	300,000 EUR	360,000 EUR
Požiarne systémy	EPS - elektronická požiarňa signalizácia SDP - skorá detekcia požiaru, IT sály SHZ - stabilné hasiace zariadenie IT sály, UPS miestnosti	400,000 EUR	480,000 EUR
Monitoring	Technologický monitoring podporných technológií DC 2 pracoviská	1,000,000 EUR	1,200,000 EUR
Projekt, inžiniering		581,450 EUR	697,740 EUR
Podporné aktivity	Projektové riadenie Publicita a informovanie	300,000 EUR	360,000 EUR
Spolu		12,510,450 EUR	15,012,540 EUR

Na základe uvedeného je odhadovaná cena projektu s využitím existujúcich priestorov 15 012 540 EUR s DPH. Cena je podobná ako cena pre DataCentrum, predpokladaným výsledkom je však o 12,5% väčšia IT plocha a niekoľkonásobne väčšia plocha pre kancelárske priestory.

4.6 Ekonomická analýza

Rozsah ekonomickej analýzy nepokrýva celú šírku aktivít spojených s budovaním budúceho dátového centra ale len prvý krok zodpovedajúci prvému plánovanému projektu a to

zabezpečenie vhodnej dátovej sály a príslušnej základnej infraštruktúry pre DataCentrum, resp. MV SR.

Analýza je vypracovaná pre oba projekty, väčšina je spoločná a len v prípade relevantných odlišností medzi projektmi DataCentra a MV SR sú tieto rozdiely uvedené.

4.6.1 Strategický kontext

Ekonomická analýza vychádza z metodiky pre CBA projektov OPIS. Prevádzkovateľom dátového centra bude DataCentrum, resp. MV SR.

Vzhľadom na charakter projektu, ktorý smeruje k poskytovaniu základnej infraštruktúry pre poskytovanie elektronických služieb jednotlivým rezortom, je pri analýze ekonomického fungovania cieľového dátového centra potrebné brať do úvahy nielen organizáciu DataCentrum, resp. Ministerstvo vnútra SR, ale aj jednotlivé prístupujúce organizácie verejnej správy. Predpokladom pre realizáciu projektu je celkový pozitívny ekonomický dopad v kontexte celej spoločnosti. Podobne to platí aj pre finančný dopad, ktorý sa v konečnom dôsledku konsoliduje v štátnom rozpočte napriek tomu, že náklady na súvisiace služby sa medzi jednotlivými organizáciami zrejme preskupia.

4.6.2 Ciele a obmedzenia

Merateľné ciele projektu musia vychádzať z hlavných cieľov projektu, ktorými sú:

- Skonsolidovať IKT infraštruktúru naprieč organizáciami tam, kde je to možné, vhodné a výhodné
- Vybudovať základnú infraštruktúru pre budúce poskytovanie služieb privátneho cloudu verejnej správy
- Zabezpečiť spoločnú prevádzku vybraných IS organizácií verejnej – primárne ide o jednoduchšie systémy a štandardné systémy, ktoré nevyžadujú komplexné špecifické know-how

Z pohľadu prvej fázy projektu, teda zabezpečenia budovy a základnej infraštruktúry pre dátové centrum je potrebné merateľné ciele prispôsobiť tomuto kontextu. Úspešnosť je teda možné definovať najmä na faktoroch:

- Zaplnenia Dátového centra infraštruktúrou pre informačné systémy verejnej správy
- Plnenia kritérií definovaných pre dostupnosť služieb Dátového centra

Konkrétne parametre cieľov budú nastavené v prípadnej žiadosti o nenávratný finančný príspevok.

Obmedzenia projektu spočívajú najmä v jeho kontexte, a to

- pokročilosť projektov OPIS, ktoré sú kandidátmi na umiestnenie do dátového centra (časový aspekt)
- technologické obmedzenia vyplývajúce zo zrejmej potreby začleniť dátové centrum do existujúcej infraštruktúry vo verejnej správe

- projektové obmedzenia súvisiace s programom OPIS, financovaním z fondov EÚ a postupov verejného obstarávania

4.6.3 Stručný popis alternatívnych riešení

Ako už štúdia popisuje existuje niekoľko alternatív spôsobu zrealizovanie dátového centra. Tieto boli vyhodnotené v kapitole 4.5.6 Cena riešenia. Na základe vyhodnotenia sa ako najvhodnejšia ukázala alternatíva kúpy existujúcich priestorov pre dátovú sálu s požadovaným technologickým vybavením pre DataCentrum a adaptácia konkrétnej budovy MV SR pre projekt tohto rezortu.

Alternatívy k realizácii takéhoto dátového centra sú nasledovné:

- Pokračovanie súčasného stavu a rozvoj existujúcich dátových sál
- Využívanie služieb komerčných dátových centier za účelom prevádzky infraštruktúry a informačných systémov verejnej správy

Druhú alternatívu je možné pomerne jednoducho vyhodnotiť ako finančne nákladnejšiu pri plánovanej životnosti projektu 15 rokov.

Ekonomická analýza sa teda zameriava na prvú alternatívu, ktorá však ako už štúdia uvádza prináša problémy s realizovateľnosťou vzhľadom na predpokladané technické a administratívne problémy pri rozvoji existujúcich dátových sál, ktoré vo väčšine prípadov nespĺňajú základné parametre kritických dátových centier a často ani neumožňujú vykonanie potrebných stavebných úprav, resp. by tieto úpravy boli spojené s neúmernými nákladmi.

Alternatívy uvažované v ekonomickej analýze sú teda:

- Pokračovanie súčasného stavu a rozvoj existujúcich dátových sál
- Zrealizovanie Dátového centra

4.6.4 Kvantitatívna analýza navrhnutého riešenia

Pre výpočet ekonomickej návratnosti projektu bola použitá cena riešenia z kapitoly 4.5.6 Cena riešenia a kalkulácia TCO z kapitoly 5.2 Kalkulácia nákladov na vlastníctvo hardvéru.

Pre alternatívu 1 boli náklady odhadnuté nasledovne:

- Predpokladá sa využitie priestoru s rovnakou úhrnnou veľkosťou plochy. Reálne sa kvôli menšej efektívnosti pri rozdelení do viac sál použije zrejme viac plochy, avšak pre potreby ekonomickej analýzy tento rozdiel nezohľadňujeme.
- Predpokladá sa približne rovnaká cena za realizáciu rovnakej plochy. Nakoľko použitý benchmark nezohľadňuje veľkosť sály, je možné tento odhad použiť. Reálne pri úpravách menších sál je potrebné počítať s vyššími nákladmi na 1 kW, istú kompenzáciu tohto faktu by však umožnilo umiestnenie menej kritických komponentov do existujúcich sál (nesplňajúcich definované parametre)
- TCO náklady budú tiež porovnateľné, nakoľko sa vychádza z pravidelnej obmeny technológií podľa ich typickej životnosti, ktorej cena sa počíta z obstarávacej ceny. Podobné náklady na energiu je možné očakávať porovnateľné

DataCentrum

Pre alternatívu 2 vzniká dodatočný finančný náklad v podobe mzdových nákladov na dodatočných zamestnancov DataCentra, kde sa predpokladá prijatie 12 zamestnancov kvôli prevádzke novej dátovej sály (číslo je zdanlivo nízke pri aktuálnom počte zamestnancov 91, neobsahuje však zamestnancov spravujúcich jednotlivé systémy, keďže tie nie sú súčasťou projektu). Vo výpočte boli použité priemerné osobné náklady z výročnej správy DataCentra za rok 2012.

Kvalitatívne prínosy alternatívy 2 nie je pre tento projekt priamo možné vyčíslieť ušetreným časom používateľa, avšak vzhľadom na predpokladanú zvýšenú dostupnosť prevádzkovaných systémov sa v malej miere dostaví aj tento efekt. Primárnym nepriamym prínosom je umožnenie zamestnancom organizácií verejnej správy, ktorých IKT a informačné systémy budú prevádzkované v Dátovom Centre, skvalitňovať služby v ich správe na vyšších úrovniach – teda samotné informačné systémy. Tento benefit bol vyčíslený odhadnutým počtom až 24 zamestnancov (po 2 zamestnancov z 12 organizácií) s postupným nábehom, pričom osobné náklady na zamestnanca boli použité podľa DataCentra, keďže ide o špecialistov v rovnakej oblasti.

Na základe vyššie uvedených parametrov je investícia z pohľadu ekonomickej čistej súčasnej hodnoty návratná v 9. roku. Nasledujúca tabuľka uvádza prehľad prínosov a čistej súčasnej hodnoty z projektu.

Tabuľka 11 - Sumárna kvantitatívna analýza nákladov a prínosov (CBA) pre projekt DataCentra

Obdobie	Čisté prínosy						Čistá súčasná hodnota z projektu			
	Finančné prínosy			Ekonomické prínosy			koeficient období	Finančná (FNPV)	Ekonomická (ENPV)	Kumulovaná diskont. návrhnosť ENPV
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel				
t1	-16,282,059.36	-16,474,059.36	-192,000.00	-16,282,059.36	-16,474,059.36	-192,000.00	0	-192,000.00	-192,000.00	-192,000.00
t2	-1,611,304.03	-1,841,826.85	-230,522.82	-1,611,304.03	-1,688,144.97	-76,840.94	1	-218,505.04	-72,835.01	-264,835.01
t3	-1,748,548.70	-1,979,071.53	-230,522.82	-1,748,548.70	-1,786,969.17	-38,420.47	2	-207,113.79	-34,518.96	-299,353.98
t4	-1,885,793.38	-2,116,316.20	-230,522.82	-1,885,793.38	-1,885,793.38	0.00	3	-196,316.39	0.00	-299,353.98
t5	-2,322,415.73	-2,552,938.55	-230,522.82	-2,322,415.73	-2,283,995.26	38,420.47	4	-186,081.88	31,013.65	-268,340.33
t6	-2,023,038.05	-2,253,560.87	-230,522.82	-2,023,038.05	-1,946,197.11	76,840.94	5	-176,380.93	58,793.64	-209,546.69
t7	-2,023,038.05	-2,253,560.87	-230,522.82	-2,023,038.05	-1,907,776.64	115,261.41	6	-167,185.72	83,592.86	-125,953.83
t8	-2,263,038.05	-2,493,560.87	-230,522.82	-2,263,038.05	-2,109,356.17	153,681.88	7	-158,469.87	105,646.58	-20,307.25
t9	-2,023,038.05	-2,253,560.87	-230,522.82	-2,023,038.05	-1,830,935.70	192,102.35	8	-150,208.41	125,173.68	104,866.43
t10	-2,416,956.05	-2,647,478.87	-230,522.82	-2,416,956.05	-2,186,433.23	230,522.82	9	-142,377.64	142,377.64	247,244.07
t11	-2,023,038.05	-2,253,560.87	-230,522.82	-2,023,038.05	-1,792,515.23	230,522.82	10	-134,955.11	134,955.11	382,199.18
t12	-2,023,038.05	-2,253,560.87	-230,522.82	-2,023,038.05	-1,792,515.23	230,522.82	11	-127,919.53	127,919.53	510,118.71
t13	-2,023,038.05	-2,253,560.87	-230,522.82	-2,023,038.05	-1,792,515.23	230,522.82	12	-121,250.74	121,250.74	631,369.45
t14	-2,023,038.05	-2,253,560.87	-230,522.82	-2,023,038.05	-1,792,515.23	230,522.82	13	-114,929.62	114,929.62	746,299.07
t15	-2,562,415.73	-2,792,938.55	-230,522.82	-2,562,415.73	-2,331,892.91	230,522.82	14	-108,938.02	108,938.02	855,237.09
SPOLU	-45,253,797.36	-48,673,116.87	-3,419,319.51	-45,253,797.36	-43,601,614.78	1,652,182.58	SPOLU	-2,402,632.69	855,237.09	

Ministerstvo vnútra SR

Kvantitatívna analýza pre MV SR stavia na rovnakých predpokladoch ako analýza pre DataCentrum. Vzhľadom na predpokladanú veľkosť cieľového dátového centra boli niektoré hodnoty proporčne navýšené – počet prijatých zamestnancov MV SR na 14 a počet zamestnancov ostatných organizácií, ktorí sú odbremenení od správy technologickej infraštruktúry cieľovo až na 28. Pre výpočet mzdových nákladov bola použitá platová tarifa štátnych zamestnancov, konkrétne platová trieda 10. Prehľad prínosov a čistej súčasnej hodnoty projektu v nasledovnej tabuľke ukazuje návratnosť investície v 9. roku.

Tabuľka 12 Sumárna kvantitatívna analýza nákladov a prínosov (CBA) pre projekt MV SR

CISTÉ PRÍNOSY	Čisté prínosy						Čistá súčasná hodnota z projektu				
	Finančné prínosy			Ekonomické prínosy			koeficient obdobia	Finančná (FNPV)	Ekonomická (ENPV)	Kumulovaná diskont. návratnosť ENPV	
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel					
Obdobie	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel					
t1	-16,344,628.20	-16,704,628.20	-360,000.00	-16,344,628.20	-16,704,628.20	-360,000.00	0	-360,000.00	-360,000.00	-360,000.00	<
t2	-1,836,838.44	-2,023,199.16	-186,360.72	-1,836,838.44	-1,916,707.32	-79,868.88	1	-176,645.23	-75,705.10	-435,705.10	<
t3	-1,981,588.68	-2,167,949.40	-186,360.72	-1,981,588.68	-2,008,211.64	-26,622.96	2	-167,436.24	-23,919.46	-459,624.56	<
t4	-2,126,338.92	-2,312,699.64	-186,360.72	-2,126,338.92	-2,073,093.00	53,245.92	3	-158,707.34	45,344.95	-414,279.61	<
t5	-2,639,057.22	-2,825,417.94	-186,360.72	-2,639,057.22	-2,559,188.34	79,868.88	4	-150,433.49	64,471.50	-349,808.11	<
t6	-2,271,089.16	-2,457,449.88	-186,360.72	-2,271,089.16	-2,164,597.32	106,491.84	5	-142,590.99	81,480.57	-268,327.55	<
t7	-2,271,089.16	-2,457,449.88	-186,360.72	-2,271,089.16	-2,137,974.36	133,114.80	6	-135,157.34	96,540.95	-171,786.59	<
t8	-2,571,089.16	-2,757,449.88	-186,360.72	-2,571,089.16	-2,411,351.40	159,737.76	7	-128,111.22	109,809.62	-61,976.98	<
t9	-2,271,089.16	-2,457,449.88	-186,360.72	-2,271,089.16	-2,084,728.44	186,360.72	8	-121,432.43	121,432.43	59,455.46	Rok návratu
t10	-2,755,257.66	-2,941,618.38	-186,360.72	-2,755,257.66	-2,568,896.94	186,360.72	9	-115,101.83	115,101.83	174,557.29	>
t11	-2,271,089.16	-2,457,449.88	-186,360.72	-2,271,089.16	-2,084,728.44	186,360.72	10	-109,101.26	109,101.26	283,658.56	>
t12	-2,271,089.16	-2,457,449.88	-186,360.72	-2,271,089.16	-2,084,728.44	186,360.72	11	-103,413.52	103,413.52	387,072.08	>
t13	-2,271,089.16	-2,457,449.88	-186,360.72	-2,271,089.16	-2,084,728.44	186,360.72	12	-98,022.29	98,022.29	485,094.37	>
t14	-2,271,089.16	-2,457,449.88	-186,360.72	-2,271,089.16	-2,084,728.44	186,360.72	13	-92,912.13	92,912.13	578,006.50	>
t15	-2,939,057.22	-3,125,417.94	-186,360.72	-2,939,057.22	-2,752,696.50	186,360.72	14	-88,068.37	88,068.37	666,074.87	>
SPOLU	-49,091,479.62	-52,060,529.70	-2,969,050.08	-49,091,479.62	-47,720,987.22	1,370,492.40	SPOLU	-2,147,133.69	666,074.87		

4.6.5 Analýza rizík

4.6.5.1 Použitá metodika

Predmetom riadenia rizík je identifikácia možných ohrození (hrozieb) pri realizácii projektu, určenie pravdepodobnosti ich výskytu a možných dopadov. Pre identifikované hrozby budú následne definované predbežné opatrenia, ktoré ohrozenia a ich dopad znížia alebo úplne eliminujú.

Analýza rizík neadresuje bezpečnostné riziká a riziká, ktoré sú relevantné pre prevádzku samotného Dátového centra, ako sú prírodné hrozby, hrozby vplyvom ľudskej činnosti, zlyhanie infraštruktúry a pod..

Pre potreby tejto štúdie bolo zvolená jednoduchá a intuitívna metodika, ktorá vychádza z 5 rôznych úrovní dopadu ohrozenia a 5 úrovní pravdepodobnosti, že ohrozenie nastane.

Tabuľka 13 – Ukazovatele dopadu ohrozenia

Úroveň	Charakteristika	Popis
1	Nevýznamný	Minimálne ohrozenie projektu, malé finančné straty, ciele nie sú ohrozené
2	Malý	Ohrozenie parciálnych cieľov projektu, stredné finančné straty, malý dopad na zákazníkov, zmena projektového plánu
3	Stredný	Niektoré parciálne ciele projektu nebudú dosiahnuté, vysoké finančné straty, významný dopad na zákazníkov, dobré meno mierne poškodené
4	Veľký	Niektoré základné ciele projektu nebudú dosiahnuté, veľké finančné straty, výrazné poškodenie dobrého mena
5	Katastrofálny	Základné ciele projektu nebudú dosiahnuté, enormné finančné straty, strata dobrého mena

Tabuľka 14 – Ukazovatele pravdepodobnosti vzniku ohrozenia

Úroveň	Charakteristika	Popis
1	Takmer isté	Očakáva sa, že nastane vo väčšine prípadov
2	Asi nastane	Vo väčšine prípadov pravdepodobne nastane
3	Možno nastane	Niekedy by azda mohlo nastať
4	Asi nenastane	Vo väčšine prípadov by nemalo nastať

5	Sotva nastane	Môže nastať iba za výnimočných okolností
---	---------------	--

Matica dopadov a pravdepodobnosti vzniku rizika definuje 4 úrovne rizika, ktoré následne určujú voľbu opatrení na jeho elimináciu, resp. zníženie.

- Extrémne riziko (E) - vyžaduje okamžitú nápravu
- Vysoké riziko (V) - treba dať do pozornosti vrcholovému manažmentu
- Stredné riziko (S) – je potrebné určiť konkrétnu zodpovednosť manažmentu
- Malé riziko (M) - riadi sa bežnými postupmi

Tabuľka 15 – Úrovne rizika

Pravdepodobnosť vzniku	Dopad					
		1 (nevýznamný)	2 (malý)	3 (stredný)	4 (veľký)	5 (katastrofálny)
	1 (takmer isté)	V	V	E	E	E
	2 (asi nastane)	S	V	V	E	E
	3 (možno nastane)	M	S	V	E	E
	4 (asi nenastane)	M	M	S	V	E
	5 (sotva nastane)	M	M	S	V	V

4.6.5.2 Projektové riziká

Ohrozenia projektu budovania dátového centra je možné rozdeliť do 3 kategórií:

- Projektové
 - Oneskorenie počas obstarania- administratíva
 - Oneskorenie počas obstarania - realizácia
 - Nedodržanie cieľov, zdrojov a termínov následného zaplňania dátového centra Časová disharmonizácia s projektmi implementácie ISVS (najmä OPIS PO1)
 - Negatívny dopad na existujúce prostredie DataCentra
- Organizačné a procesné
 - Strata financovania pre ďalšie fázy projektu
 - Strata trvalej udržateľnosti
 - Nízka akceptácia DataCentra ako centrálného poskytovateľa služieb dátového centra
 - Nedostatočné skúsenosti a odborná úroveň personálu Dátového centra
- Technologické
 - Strata interoperability

Oneskorenie počas obstarania - administratíva

Pravdepodobnosť: možno nastane

Dopad: veľký

Úroveň rizika: extrémne riziko

- Popis:* Doterajšie skúsenosti s obstarávaním komplexných projektov v oblasti IKT sa spájajú s výraznými oneskoreniami prípadne opakovanými vyhláseniami súťaže.
- Opatrenia:* Je potrebné sa detailne venovať príprave verejného obstarania a spolupracovať pri vypracovaní súťažných podkladov s Riadiacim orgánom OPIS.

Oneskorenie počas obstarania - realizácia

- Pravdepodobnosť:* možno nastane
- Dopad:* veľký
- Úroveň rizika:* extrémne riziko
- Popis:* Obstarávaná dátová sála a jej infraštruktúra musí splniť mnoho náročných parametrov. Niektorí prípadní uchádzači, resp. ich dátové centrá môžu vyžadovať dodatočné úpravy pred odovzdaním priestorov, ktorých nezvládnutie môže viesť k významnému oneskoreniu až strate financovania
- Opatrenia:* Je potrebné dôkladne zmluvne ošetriť očakávanie od víťaza prípadného tendra a definovať opatrenia pre ich priebežné vyhodnocovanie.

Nedodržanie cieľov, zdrojov a termínov následného zaplňania dátového centra

- Pravdepodobnosť:* možno nastane
- Dopad:* veľký
- Úroveň rizika:* extrémne riziko
- Popis:* Vybudovanie Dátového centra je náročný a komplexný projekt, ktorý vyžaduje rigidné projektové riadenie a silnú, priebežnú koordináciu všetkých dodávateľov. V opačnom prípade hrozí nedodržanie cieľov, termínov a/alebo navýšenie rozpočtu. Pre aktuálnu fázu projektu (budova a základná infraštruktúra) je však vzhľadom na nízku komplexnosť toto riziko pomerne malé. Rizikom pre zriadenie dátovej sály je možné neplnenie prípadných kritérií jej efektívneho využívania.
- Opatrenia:* Využiť služby skúseného integrátora, ktorý zabezpečí kvalitu projektových dodávok.

Časová disharmonizácia s projektmi implementácie ISVS (najmä OPIS PO1)

- Pravdepodobnosť:* možno nastane
- Dopad:* veľký
- Úroveň rizika:* extrémne riziko
- Popis:* Projekt Dátového centra musí byť ukončený tak, aby ním poskytované služby boli reálne využiteľné pre definované ISVS. V opačnom prípade budú musieť jednotliví správcovia ISVS projekty riešiť IKT infraštruktúru individuálne čím im vzniknú dodatočné náklady a na strane Dátového centra dôjde k zásadnému ovplyvneniu predpokladanej návratnosti.
- Opatrenia:* Detailne analyzovať požiadavky projektov správcov ISVS a vzájomne koordinovať projektové plány všetkých zúčastnených strán. V prípade konfliktov pripraviť náhradné (dočasné) scenáre.

Negatívny dopad na existujúce prostredie DataCentra

Pravdepodobnosť: možno nastane

Dopad: stredný

Úroveň rizika: vysoké riziko

Popis: Projekt budovania Dátového centra si vyžiada zásah do prostredia DataCentra vo všetkých oblastiach (organizačná, technologická, legislatívna, ...).

Opatrenia: Dôsledné dodržanie procesu riadenia zmien, vrátane dôkladnej analýzy dopadov a prípravy náhradných, resp. back-out scenárov. Vyhodnotenie každej zmeny z pohľadu dopadu na existujúce prostredie a priebežné zapracovanie nápravných opatrení.

Strata financovania pre ďalšie fázy projektu

Pravdepodobnosť: asi nenastane

Dopad: veľký

Úroveň rizika: vysoké riziko

Popis: Ďalšie fázy budovania logického dátového centra verejnej správy budú vyžadovať značné finančné prostriedky, či už zo štátneho rozpočtu alebo štrukturálnych fondov EU. V prípade, že tieto prostriedky nebudú k dispozícii, zníži sa efektivita tejto investície.

Opatrenia: Presadzovať stratégiu budovania logického dátového centra na najvyšších úrovniach a zapracovať ju do strategických dokumentov pre informatizáciu.

Strata trvalej udržateľnosti

Pravdepodobnosť: možno nastane

Dopad: veľký

Úroveň rizika: extrémne riziko

Popis: Nedostatok prostriedkov na prevádzku systému bude ohrozovať trvalú udržateľnosť vybudovaného Dátového centra. Nedodržanie podmienok udržateľnosti OPIS by viedlo k vráteniu poskytnutého NFP.

Opatrenia: Prehodnotiť prostriedky na údržbu a prevádzku Dátového centra po skončení projektu. Potrebne náklady zahrnúť do prípravy rozpočtu MF SR v nasledujúcich obdobiach.

Nízka akceptácia DataCentra ako centrálného poskytovateľa služieb dátového centra

Pravdepodobnosť: možno nastane

Dopad: veľký

Úroveň rizika: vysoké riziko

Popis: Dátové centrum ako poskytovateľ dátových služieb pre systémy zabezpečujúce eGovernment služby by mal byť verejnou správou akceptovaný ako dôveryhodný, stabilný a finančne efektívny partner. V opačnom prípade to môže vyvolať rezistenciu jednotlivých rezortov voči využívaniu služieb Dátového centra a snahu riešiť oblasť IKT infraštruktúry individuálne čím dôjde k celkovému zníženiu efektivity prevádzky IKT infraštruktúry vo verejnej správe.

Opatrenia: Na strane Dátového centra zabezpečiť a priebežne sledovať požadované parametre poskytovaných služieb. Na strane riadiacich orgánov OPIS vynútiť zohľadnenie existencie centrálného poskytovateľa služieb dátového centra pri príprave a implementácii projektov. Na strane Ministerstva financií SR, resp. Ministerstva vnútra SR predloženie návrhu legislatívy upravujúcej povinnosť využívania Dátového centra.

Nedostatočné skúsenosti a odborná úroveň personálu Dátového centra

Pravdepodobnosť: možno nastane

Dopad: malý

Úroveň rizika: stredné riziko

Popis: Zníženie dostupnosti a kvality IKT infraštruktúry.

Opatrenia: Poskytnúť potrebné školenie a tréning. Zabezpečiť priebežné vzdelávanie.

Strata interoperability

Pravdepodobnosť: asi nenastane

Dopad: stredný

Úroveň rizika: stredné riziko

Popis: Rozsah a efektivita využívania služieb Dátového centra závisí na technologickej interoperabilite.

Opatrenia: V technickej a technologickej oblasti je nutné dôsledne vyžadovať dodržiavanie otvorených a neutrálnych štandardov.

4.6.6 Nefinančné prínosy a náklady

Implementácia projektu prináša niekoľko pozitív, ktoré nie je možné priamo finančne vyčíslieť, sú však dôležité pre poskytovanie elektronických služieb verejnosti aj ďalší koncepčný rozvoj IKT vo verejnej správe smerom k moderným postupom a technológiám.

- Vyššia dostupnosť elektronických služieb
 - Je predpokladaným výsledkom budovania väčšieho dátového centra s geograficky oddelenými lokalitami a vysokým stupňom redundancie komponentov, že dokáže zabezpečiť vyššiu dostupnosť prevádzkovaných systémov ako jednotlivé menšie dátové centrá budované jednotlivými rezortmi resp. organizáciami verejnej správy. Tento prínos nie je možné priamo vyčíslieť, ma však priamy dopad na reputáciu IT vo verejnej správe medzi odbornou i širokou verejnosťou a efektivitu využívania pracovného času zamestnancami organizácií verejnej správy aj verejnosti
- Vyššia odbornosť zamestnancov zodpovedných za prevádzku informačných systémov
 - Pri prevádzke väčšieho dátového centra získajú zamestnanci DataCentra, resp. MV SR, oveľa bohatšie skúsenosti ako zamestnanci organizácií s relatívne menšími dátovými centrami, keďže toto väčšie riešenie umožňuje oveľa väčšiu špecializáciu zamestnancov (bez potreby riešenia iných, často podružných činností) a pri väčšom portfóliu obsluhovaných systémov aj oveľa lepšie budovanie vedomostnej základne pre riešenie budúcich úloh resp. problémov
- Príprava na budovanie cloudu verejnej správy

- Pre vybudovanie platforiem pre cloud sú potrebné značné investície, pričom investícia riešená v tomto dokumente je len jedna z nutných investícií na ceste k plnohodnotnému cloud riešeniu pre verejnú správu. Po dobudovaní cloud infraštruktúry a začatí poskytovania služieb sa umožní nová úroveň efektivity dynamickým riadením zdrojov pre jednotlivé informačné systémy, s plným využitím virtualizácie a efektívnym spravovaním potrebných výkonových rezerv.
- Lepšia škálovateľnosť a efektívnosť využitia IKT vo verejnej správe
 - Realizovanie zmien vo veľkom dátovom centre je oproti niekoľkým malým jednoduchšie a dovoľí šetriť čas aj prostriedky a minimalizovať výpadky systémov pri zmenách. Tam, kde v malom dátovom centre je už potrebné riešiť jeho rozšírenie aj pri relatívne malom náraste požiadaviek by veľké dátové centrum malo ponúknuť škálovateľnosť v rámci jedného dátového centra a prípadne aj dočasnú infraštruktúru tam, kde je to potrebné kvôli veľkosti, resp. charakteru zmeny.

4.7 Návrh projektového zámeru

Cieľom projektu bezprostredne vyplývajúcim z tejto štúdie je zriadenie budovy dátového centra so základnou infraštruktúrou pre sieťovú konektivitu, napájanie, chladenie a bezpečnosť v zmysle požiadaviek a špecifikácií uvedených v predchádzajúcich kapitolách.

Tomuto cieľu sú prispôsobené aktivity, ktoré z pohľadu žiadateľa/prijímateľa v tomto projekte sú pomerne priamočiare a sú zjednodušené na obstaranie predmetnej budovy a podporné projektové aktivity súvisiace jednak z obstarávaním a jednak riadením projektu vzhľadom na začlenenie projektu do OPIS.

4.7.1 Príprava projektu

V príprave projektu sú zásadné 2 faktory, ktoré okrem vecnej musia byť dôkladne zvládnuté aj po formálnej stránke:

- Príprava dokumentácie pre obstarávanie budovy dátového centra DataCentra, resp. pre stavebné a technologické úpravy budovy v prípade MV SR
- Príprava projektovej dokumentácie a formálnych náležitostí vyplývajúcich z OPIS – Žiadosť o NFP vrátane všetkých príloh a príprava zmluvy o poskytnutí NFP.

4.7.2 Metodika riadenia

Riadenie projektu bude realizované v súlade so všeobecne akceptovanými metodikami projektového riadenia. Bude napĺňať požiadavky riadenia projektu stanovené vo výzve na predloženie ŽoNFP a Štandardom pre riadenie informačno – technologických projektov stanovených výnosom MF SR č. 312/2010 Z.z. o štandardoch pre informačné systémy verejnej správy.

Popísaná metodika sa opiera o metodiku PRINCE 2, ktorá rozsahom svojho využívania vo svete predstavuje nepísaný štandard v danej oblasti. PRINCE alebo „Projects IN Controlled Environments” (projekty v riadenom prostredí) predstavuje procesne orientovanú metodiku riadenia projektov, ktorá obsahuje štruktúrovaný postup zahŕňajúci riadenie, kontrolu a

organizáciu projektu. PRINCE2® je ochrannou známkou OGC (Office of Government Commerce), ktorý je súčasťou Britského ministerstva financií.

Metodika riadenia projektu, v zmysle princípov PRINCE2, je zostavená z troch základných prvkov:

- komponentov
- procesov
- techník

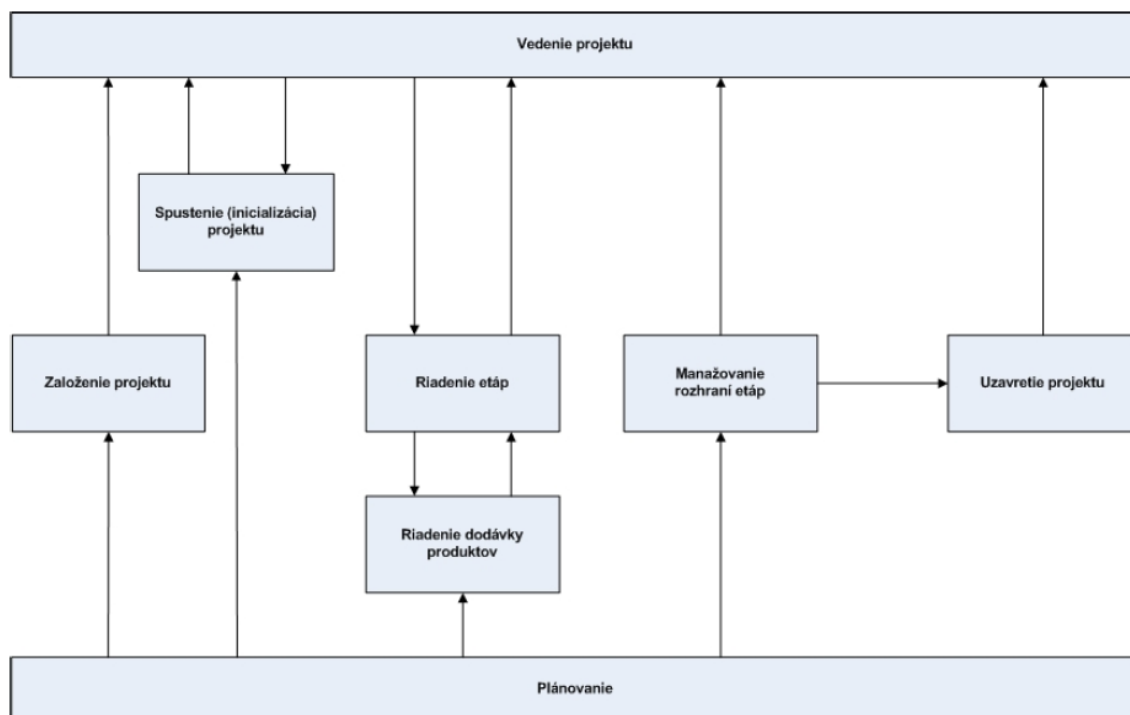
Prostredníctvom komponentov sú popísané a vysvetlené hlavné elementy projektového manažmentu a ich vzájomné prepojenie. Tieto komponenty predstavujú základné „stavebné kamene“ projektového manažmentu, vrátane manažmentu kvality a manažmentu rizík v prostredí projektu.

Definované sú nasledovné komponenty:

- Organizácia
- Plánovanie
- Riadenie
- Etapy
- Manažment rizík
- Kvalita v prostredí riadenia projektu
- Konfiguračný manažment
- Riadenie zmien

Procesy predstavujú samotný procesný model metodiky, ktorý popisuje použitie jednotlivých komponentov metodiky s účelom dosiahnutia plánovaných projektových cieľov. Definovaných je 8 základných procesov:

- Otvorenie projektu
- Inicializácia projektu
- Riadenie etáp
- Manažovanie dodávky projektových výstupov
- Manažovanie rozhraní etáp
- Plánovanie
- Vedenie projektu
- Uzavretie projektu



PRINCE2 definuje dve techniky:

- Produktovo-orientované plánovanie
- Vyhodnocovanie kvality

4.7.3 Harmonogram projektu

Nasledujúce tabuľky obsahujú rámcový plán projektových aktivít zvlášť pre projekt DataCentra a MV SR z dôvodu významne odlišného spôsobu realizácie týchto dvoch projektov. Stĺpce označené ako „M“ a číslo označujú mesiac od zahájenie projektových aktivít. Oba plány počítajú s paralelizáciou niektorých aktivít a relatívne bezproblémovým priebehom. Problémy v ktorýchkoľvek aktivitách, ale najmä pri obstarávaní procese, môžu viesť k predĺženiu tohto projektu.

Aktivita projektu	M1	M2	M3	M4	M5	M6
Vypracovanie projektu						
Obstaranie						
Vyhlasenie súťaže						
Predloženie ponúk uchádzačov						
Vyhodnotenie súťaže a podpis zmluvy						
Realizácia a preberanie						
Príprava dátovej sály na prebratie						
Preberacie konanie						
Spustenie do prevádzky						

Obrázok 10 Rámcový harmonogram projektu pre DataCentrum

Aktivita projektu	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Vypracovanie projektu												
Zabezpečenie príslušných povolení												
Priprava/uvoľnenie priestorov												
Stavebné úpravy												
Obstaranie stavebných úprav												
Realizácia stavebných úprav												
Technologická časť												
Obstaranie technologických dodávok												
Rozvody												
Inštalácia technológií												
Oživenie												
Spustenie do prevádzky												

Obrázok 11 Rámcový harmonogram projektu pre MV SR

5 Prílohy

5.1 **Kalkulácia celkových nákladov na vlastníctvo softvéru (TCO)**

Vzhľadom na charakter projektu, kde softvér nie je súčasťou riešenia, kalkulácia nie je uvedená.

5.2 **Kalkulácia nákladov na vlastníctvo hardvéru**

Kalkulácia využíva upravenú šablónu vzhľadom na fakt, že štruktúra projektových nákladov a ďalších nákladov životného cyklu nie je kompatibilná so štruktúrou používaných pre projekty informačných systémov a elektronických služieb.

Tabuľka 16 Kalkulácia pre projekt DataCentra

Kategória	Podkategória	projekt	rok 1	rok 2	rok 3	rok 4	rok 5	rok 6	rok 7	rok 8	rok 9	rok 10	rok 11	rok 12	rok 13	rok 14	rok 15
		% z obstarávacej ceny	cena														
budova	obstaranie	20%	2468000.00														
	servis			131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00
napájanie	obnova							52,522.40				52,522.40					52,522.40
	obstaranie	50%	6170000.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00	328,265.00
chladenie	obnova							196,959.00		200,000.00		196,959.00					396,959.00
	obstaranie	20%	2468000.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00	131,306.00
bezpečnosť	obnova											78,783.60					
	obstaranie	10%	1234000.00														
	servis			65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00	65,653.00
	obnova							39,391.80				39,391.80					39,391.80
Spolu bez DPH		100%		656,530.00	656,530.00	656,530.00	656,530.00	906,011.40	656,530.00	656,530.00	856,530.00	656,530.00	984,795.00	656,530.00	656,530.00	656,530.00	1,106,011.40
Energie				50%	60%	70%	80%	90%	90%	90%	90%	90%	90%	90%	90%	90%	90%
Obsadenosť IT [kW]				320	384	448	512	576	576	576	576	576	576	576	576	576	576
poplatky		EUR/kWh		571,852.80	686,223.36	800,593.92	914,964.48	1,029,335.04	1,029,335.04	1,029,335.04	1,029,335.04	1,029,335.04	1,029,335.04	1,029,335.04	1,029,335.04	1,029,335.04	1,029,335.04
Spolu s DPH			14808000	1474059.4	1611304	1748548.7	1885793.4	2322415.728	2023038.048	2023038.048	2263038.048	2023038.048	2416956.048	2023038.048	2023038.048	2023038.048	2562415.728

Tabuľka 17 Kalkulácia pre projekt MV SR

Kategória	Podkategória	projekt	rok 1	rok 2	rok 3	rok 4	rok 5	rok 6	rok 7	rok 8	rok 9	rok 10	rok 11	rok 12	rok 13	rok 14	rok 15
		% z obstarávacej ceny	cena														
budova	obstaranie	20%	2442090.00														
	servis			161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50
konektivita	obnova							64,555.80				64,555.80					64,555.80
	obstaranie																
napajanie	obnova																
	obstaranie	50%	6105225.00														
chladenie	obnova			403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75	403,473.75
	obstaranie	20%	2442090.00					242,084.25		250,000.00		242,084.25					492,084.25
bezpecnost	obnova			161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50	161,389.50
	obstaranie	10%	1221045.00										96,833.70				
	servis			80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75	80,694.75
	obnova							48,416.85				48,416.85					48,416.85
Spolu		100%	12210450.00	806,947.50	806,947.50	806,947.50	806,947.50	1,113,587.55	806,947.50	806,947.50	1,056,947.50	806,947.50	1,210,421.25	806,947.50	806,947.50	806,947.50	1,363,587.55
Energie				50%	60%	70%	80%	90%	90%	90%	90%	90%	90%	90%	90%	90%	90%
Obsadenosť IT [kW]				337.5	405	472.5	540	607.5	607.5	607.5	607.5	607.5	607.5	607.5	607.5	607.5	607.5
poplatky		EUR/kWh		603,126.00	723,751.20	844,376.40	965,001.60	1,085,626.80	1,085,626.80	1,085,626.80	1,085,626.80	1,085,626.80	1,085,626.80	1,085,626.80	1,085,626.80	1,085,626.80	1,085,626.80
Spolu s DPH			14652540	1692088.2	1836838.4	1981588.7	2126338.9	2639057.22	2271089.16	2271089.16	2571089.16	2271089.16	2755257.66	2271089.16	2271089.16	2271089.16	2939057.22